VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH PŘÍSTUPOVÉHO SYSTÉMU JAKO SOUČÁST ŘEŠENÍ FYZICKÉ BEZPEČNOSTI

DESIGN OF ACCESS SYSTEM AS A PART OF PHYSICAL SECURITY SOLUTION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Ing. Matěj Dohnal**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Ing. Matěj Dohnal**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Návrh přístupového systému jako součást řešení fyzické bezpečnosti

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Pro vybranou společnost na základě analýzy rizik vypracujte návrh přístupového systému v rámci fyzické bezpečnosti ISMS.

Základní literární prameny:

ČSN ISO/IEC 27001, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky. Praha: Český normalizační institut, 2014.

ČSN ISO/IEC 27002, Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Soubor postupů. Praha: Český normalizační institut, 2014.

DOUCEK, Petr. Řízení bezpečnosti informací: 2. rozšířené vydání o BCM. 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-80-7431-050-8.

ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17.

V Brně, dne 28. 2. 2017

L. S.

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

doc. RNDr. Bedřich Půža, CSc.	doc. Ing. et Ing. Stanislav Škapa, Ph.D.
ředitel	děkan

Abstrakt

Tato diplomová práce pracovává návrh přístupového systému jako součásti řešení fyzické bezpečnosti pro energetickou společnost v České republice. Přístupový systém je navržen tak, aby vyhověl všem zákonným požadavkům, a obstál i při certifikaci dle normy ISO 27001. Nasazení navrženého přístupového systému je předvedeno na vybraném objektu společnosti, který je reprezentativní ukázkou spojení prvku kritické infrastruktury a běžného objektu společnosti.

Abstract

This master's thesis deals with design of an access system as a part of physical security solution for an energy company in the Czech Republic. The access system is designed to meet all legal requirements and conform to ISO 27001 certification. Implementation of the proposed access system is demonstrated on the selected company object, a representative example of connecting the critical infrastructure element and the company's common facility.

Klíčová slova

ISMS, Čipová karta, ISO/IEC 27000, přístupový systém, fyzická bezpečnost, bezpečnost, energetika, kritická infrastruktura, analýza rizik, opatření

Keywords

ISMS, Smart Card, ISO/IEC 27000, Access Control System, Physical security, Security, Energetics, Critical Infrastructure, Risk analysis, measures

Bibliografická citace

DOHNAL, M. *Návrh přístupového systému jako součást řešení fyzické bezpečnosti*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 129 str. Vedoucí diplomové práce Ing. Petr Sedlák.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracoval jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušil autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 26. května 2017

……...

Matěj Dohnal

Poděkování

Touto cestou bych rád poděkoval všem, kteří mě při vypracování této diplomové práce podporovali, především pak panu Ing. Petru Sedlákovi za všechny jeho rady a neutuchající víru, dále pak kolegům a nadřízeným v práci za pochopení naléhavé nutnosti psát tuto práci. Dále bych rád poděkoval Zbyškovi Vodovi a svojí rodině za pomoc při digitalizaci plánů budov. Nakonec bych rád poděkoval společnosti, jejíž jméno zde nemůže být uvedeno, a jejím zaměstnancům za poskytnutí značného množství interních materiálů potřebných nebo nápomocných pro vypracování této práce.

Obsah

Úvod

Informační bezpečnost je v poslední době stále více skloňovaným tématem, zvláště v souvislosti s úniky citlivých dat či ztrátami dat obecně. Jednou ze součástí informační bezpečnosti je i fyzická bezpečnost objektů, v nichž se informace či jiná důležitá aktiva nacházejí. Dále je tu relativně nový kybernetický zákon, který ukládá povinnost chránit prvky kritické infrastruktury státu předepsaným způsobem. Je tak trochu naším národním specifikem, že některé společnosti, ba i státní složky se snaží tvrdit, že jimi spravované zařízení či systém není kritickou infrastrukturou, i když realita je opačná. Proto patří společnosti, pro niž je tato práce zpracována, všechna čest, že se k této povinnosti staví čelem a nesnaží se z ní nijak vykrucovat.

Jak už z názvu práce vyplývá, bude se zabývat návrhem přístupového systému jakožto součásti fyzické bezpečnosti. Práce je rozdělena do 5 kapitol, kdy kapitola 1 blíže vymezuje cíl práce a upřesňuje požadavky dané zadáním.

Druhá kapitola se zabývá teoretickými východisky práce. Vyjmenovává související platné zákony a vyhlášky, jež bude muset přístupový systém respektovat, dále představuje mezinárodní i národní normy, jimž bude muset odpovídat. Nakonec se detailně věnuje procesu řízení rizik a krátce zpracovává i řízení přístupu.

Třetí kapitola analyzuje současný stav. Nejprve představuje společnost, pro niž je práce zpracovávána a zasazuje ji do kontextu zákonů a norem jmenovaných a popisovaných v kapitole předchozí. Snaží se klasifikovat objekty vlastněné společností a na základě společných znaků je rozdělit do tříd. Následují analýzy vnějšího i vnitřního prostředí společnosti, jsou vyjmenována některá rizika současného stavu.

Kapitola s pořadovým číslem 4 přináší nejprve obecný návrh přístupového systému včetně posouzení použití různých identifikátorů pro přístup. Přístupový systém je zvlášť navrhován pro jednotlivé třídy objektů společnosti. Dále jsou vyjmenována režimová opatření související s přístupovým systémem. Nakonec je nasazení systému demonstrováno na vybraném Modelovém objektu.

Kapitola 5 shrnuje přínos práce pro danou společnost. Následuje seznam zdrojové a citované literatury, seznam použitých zkratek, obrázků a tabulek. V přílohové části jsou uvedeny především kvalitativní požadavky na technická opatření fyzické ochrany.

1 Vymezení problému a cíle práce

Hlavním cílem této diplomové práce je vypracovat obecný návrh přístupového systému v rámci fyzické bezpečnosti ISMS pro vybranou společnost. Pomocí tohoto systému bude řízen přístup k aktivům společnosti, z nichž některá jsou zařazena jako prvky kritické infrastruktury dle krizového zákona a jeho prováděcích předpisů.

Společnost potřebuje nový přístupový systém jednak proto, aby jako subjekt kritické infrastruktury vyhověla legislativním požadavkům na ochranu prvků kritické infrastruktury, ale i proto, aby lépe chránila svá ostatní aktiva (majetek i zaměstnance).

Cílem práce je navrhnout obecný přístupový systém takový, aby vyhověl legislativním požadavkům na ochranu kritické infrastruktury a zároveň byl použitelný i ve všech ostatních objektech dané společnosti.

Vytvořený obecný návrh pak bude konkretizován pro jeden nebo více vybraných modelových objektů, aby se ukázalo jeho praktické nasazení. Podle těchto pilotních objektů pak bude systém nasazen ve všech objektech společnosti. Musí proto být navržený tak, aby mohl být zaváděn postupně. Zároveň by systém měl být navržen tak, aby dokázal využít co nejvíce stávajících komponent.

Navržený přístupový systém musí odpovídat ISMS dle norem řady ČSN ISO/IEC 27000, aby při případné certifikaci společnosti již nemusel být přepracováván.

2 Teoretická východiska

Tato část práce se zaměřuje na přiblížení základních teoretických východisek pro návrh přístupového systému jako součásti řešení fyzické ochrany. Budou uvedeny základní předpisy, doporučení a metodiky vtahující se k fyzické bezpečnosti. Fyzická bezpečnost je jednou ze součástí daleko širšího oboru informační bezpečnosti organizace, případně i kybernetické bezpečnosti. Vycházet budeme z norem vztahujících se k Systému řízení bezpečnosti informace (ISMS – Information Security Management System), mimo to, jelikož se jedná o energetickou společnost, budou zmíněny i patřičné zákony regulující toto odvětví. Dále budou zmíněny normy a zákony hovořící o Kritické Infrastruktuře České republiky, jimiž se budeme muset rovněž při návrhu přístupového systému zcela jistě řídit, aby jim bylo rovněž vyhověno.

2.1 Slovník základních pojmů

Následující tabulka uvedená v této podkapitole si klade za cíl být základním, nikoli vyčerpávajícím přehledem pojmů použitých v této práci. Jejich výklad vychází z platných norem řady ČSN ISO/IEC 27000:2017 (1) a některých zákonů.

Název	Výklad
Aktivum	Aktivum je cokoli, co má pro organizaci ochranu a co tedy vyžaduje ochranu (2)
Analýza rizika	Proces pochopení povahy rizika a určení úrovně rizika (1)
Audit	Systematický, nezávislý a dokumentovaný proces k získání důkazů z auditu, a jejich objektivní ohodnocení, aby se určil rozsah, v jakém jsou auditní kritéria splněna (1)
Bezpečnost informací	Zachování důvěrnosti, integrity a dostupnosti informací (1)
Distribuční soustava	Soustava vzájemně propojených vedení o napětí 110 kV (kromě těch, která jsou součástí přenosové soustavy) a vedení a zařízení o napětí 0,4/0,23 kV až 35 kV sloužící k zajištění distribuce elektřiny na vymezeném území ČR, včetně měřící techniky a elektrických přípojek. (3)
Dostupnost	Přístupnost a použitelnost na žádost oprávněné entity (1)
Důvěrnost	Vlastnost, že informace není dostupná nebo není odhalena neoprávněným jednotlivcům, entitám nebo procesům (1)
Fyzická ochrana	Technická a režimová opatření a fyzická ostraha, jejichž cílem je snížení rizika narušení funkce prvku kritické infrastruktury vyplývajícího z neoprávněných činností s majetkem, nebo zajištění bezpečnostních hrozeb (4)

Název	Výklad
Fyzická ostraha	Bezpečnostní služby vykonávané bezpečnostními pracovníky/strážnými (4)
Hrozba	Potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace (1)
Kritická infrastruktura	Prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu (4)
Kybernetický zákon	Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (5)
Incident	Nežádoucí nebo neočekáváná událost která může s významnou pravděpodobností vyvolat ohrožení bezpečnosti informací (1)
Informace (dokumentované)	Informace, které má organizace řídit a udržovat, včetně médií, na kterých jsou uloženy (1)
Informační systém	Aplikace, služby, aktiva informační technologie nebo další komponenty zacházející s informacemi (1)
Integrita	Vlastnost přesnosti a úplnosti (1)
ISMS	Systém řízení bezpečnosti informací (1)
Neshoda	Nesplnění požadavků (1)
Opatření	Prostředky modifikující riziko (1)
Organizace	Osoba nebo skupina osob, které mají své vlastní funkce s odpovědnostmi, pravomocemi a vztahy, pomocí nichž mohou dosáhnout svých cílů (1)
Perimetr	Prostorově, funkčně nebo technicky vymezená hranice objektu (např. plot, plášť budovy) (4)
Proces	Soubor aktivit majících vzájemný vztah nebo vzájemně na sebe působících a přeměňujících vstupy na výstupy (1)
Prvek KI	Zejména stavba, zařízení prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií (4) (5) (6)
Přenosová soustava	Vzájemně propojený soubor vedení a zařízení 400 kV, 220 kV a vybraných vedení 110 kV (3)
Přístupový systém	Zde chápáno jako Systém kontroly vstupu v kombinaci s mechanickými zábrannými prostředky a poplachovým, zabezpečovacím a tísňovým systémem dle ČSN P 73 4450-1 (4)
Riziko	Účinek nejistoty na dosažení cílů (1)

Název	Výklad
Řízení přístupu	Prostředky zajišťující, aby přístup k aktivům byl autorizován a omezen na základě obchodních a bezpečnostních požadavků (1)
Shoda	Splnění požadavku (1)
Subjekt KI	Provozovatel prvku KI (7)
Událost	Výskyt nebo změna určité množiny okolností (1)
Útok	Pokus o zničení, vystavení hrozbě, změnu, vyřazení z činnosti nebo získání neoprávněného přístupu k aktivu nebo uskutečnění neoprávněného použití aktiva (1)
Zranitelnost	Slabé místo aktiva nebo opatření, které může být využito jednou nebo více hrozbami (1)

Tab. 1: Slovník základních pojmů

2.2 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací (Information Security Management System), dále jen ISMS je jedním z několika celosvětově uznávaných systémů k zavedení řízení bezpečnosti. Požadavky pro jeho zavedení jsou definovány v normě ČSN ISO/IEC 27001/2013 (8). Dalšími systémy řízení bezpečnosti informací jsou knihovna ITIL Security Management případně rámec COBIT.

Co je to ISMS? Norma ČSN ISO/IEC 27000 doslova říká, že se skládá z *„politik, postupů, směrnic a příslušných zdrojů a činností, které organizace řídí, aby zajistila ochranu informačních aktiv. ISMS představuje systematický přístup k ustavení, implementování, provozování, monitorování, přezkoumávání, udržování a zlepšování bezpečnosti informací organizace tak, aby byly dosaženy její cíle. Je založen na posuzování rizik […].“* (9)

2.3 Normy řady ISO/IEC 27000

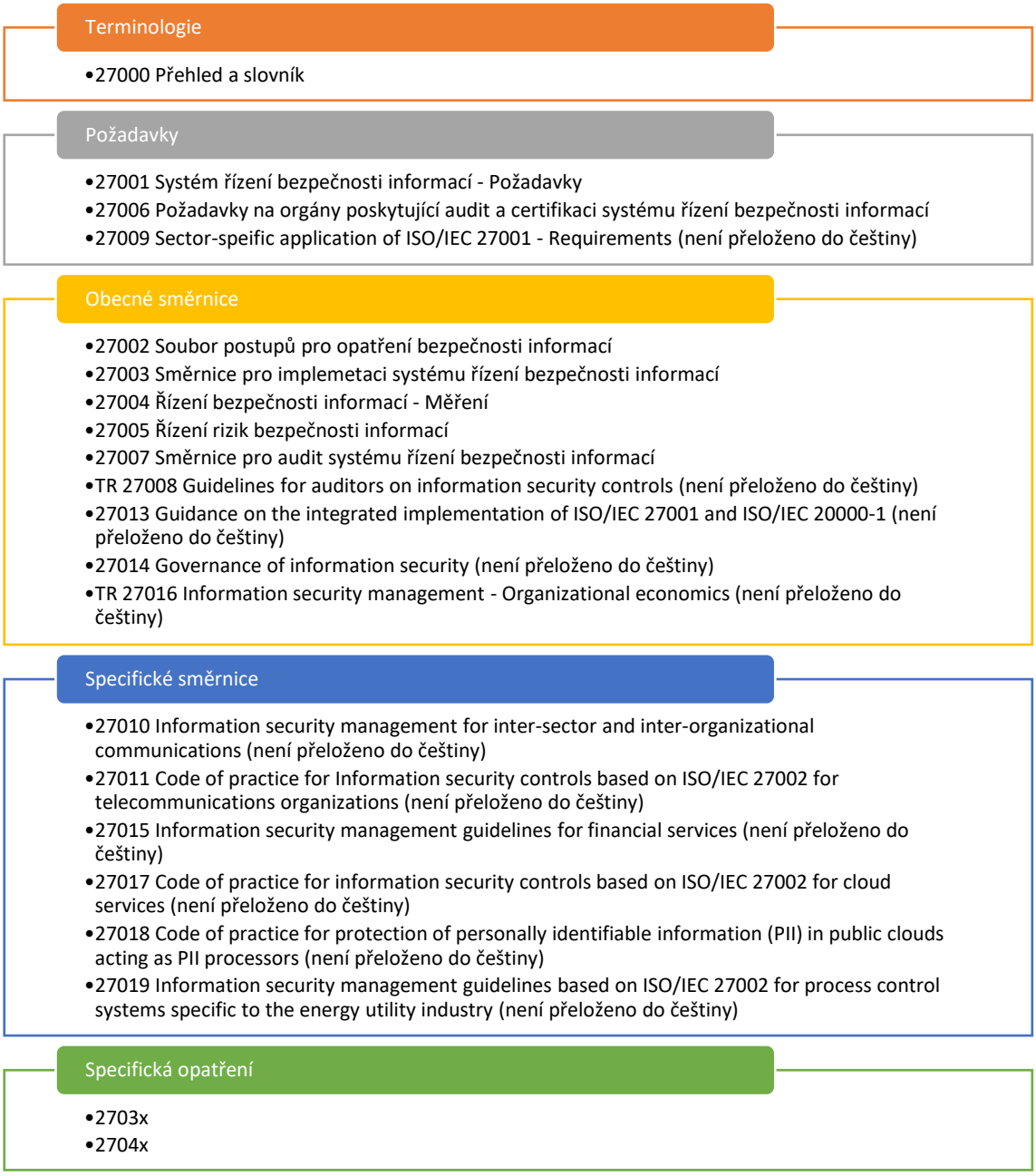
Normy řady ISO/IEC 27000 řeší standardizaci systémů řízení bezpečnosti informací (ISMS). Na vypracování mezinárodních norem se podílejí jednotliví členové organizací ISO (Mezinárodní organizace pro normalizaci) nebo IEC (Mezinárodní elektrotechnická komise) prostřednictvím technických komisí ustavených příslušnými organizacemi pro jednotlivé obory technické činnosti. (8) (10)

Překlad norem do českého jazyka zajišťuje Úřad pro technickou normalizaci, metrologii a státní zkušebnictví. Mezinárodní označení norem je pro Českou republiku převzato

a doplněno zkratkou ČSN (označení pro *Českou technickou normu* chráněné dle §4 zákona č. 22/1997 Sb.). Původně toto označení znamenalo *Česká státní norma*, později *Československá norma*, nyní *Česká technická norma*. Můžeme se setkat i s nesprávným výkladem ve znění *Česká soustava norem.* (11) (10)

2.3.1 Norma ČSN ISO/IEC 27000

V současné době platná norma ČSN ISO/IEC 27000:2014 podává přehled termínů a jejich definic platný ve všech ostatních normách řady ISO/IEC 27000, dále stručně uvádí do problematiky ISMS a přidává základní přehled norem řady ISO/IEC 27000. Norma je použitelná pro všechny typy a velikosti organizací, ať už se jedná o obchodní podniky, vládní úřady nebo neziskové organizace. (9) Strukturu norem řady ISO/IEC 27000 ilustruje tabulka na Obr. 1.



Obr. 1: Struktura řady norem ISO/IEC 27000. Upraveno dle (1) a (12).

Od 1. června 2017 vstupuje v platnost čtvrté vydání ČSN ISO/IEC 27000:2017, které nahrazuje předchozí třetí vydání z roku 2014. Hlavní změnou je zařazení do seznamu norem ISMS aktualizované a nově vydané normy. (1)

2.3.2 Norma ČSN ISO/IEC 27001

Aktuální vydání z roku 2014 nahrazuje ČSN ISO/IEC 27001:2006, která původně vzešla z ČSN BS 7799-2:2004. (13) *„Mezinárodní norma ISO/IEC 27001 byla připravena, aby*

poskytla požadavky na ustavení, implementování, udržování a neustálé zlepšování systému řízení bezpečnosti informací. Přijetí systému řízení bezpečnosti informací organizace je pro organizaci strategickým rozhodnutím. Ustavení a implementace systému řízení bezpečnosti informací organizace jsou ovlivněny potřebami a cíli organizace, požadavky na bezpečnost, používanými procesy a velikostí a strukturou organizace. […] Tato mezinárodní norma může být použita interními a externími stranami k posouzení schopnosti organizace splnit její vlastní požadavky na bezpečnost informací.“ (8)

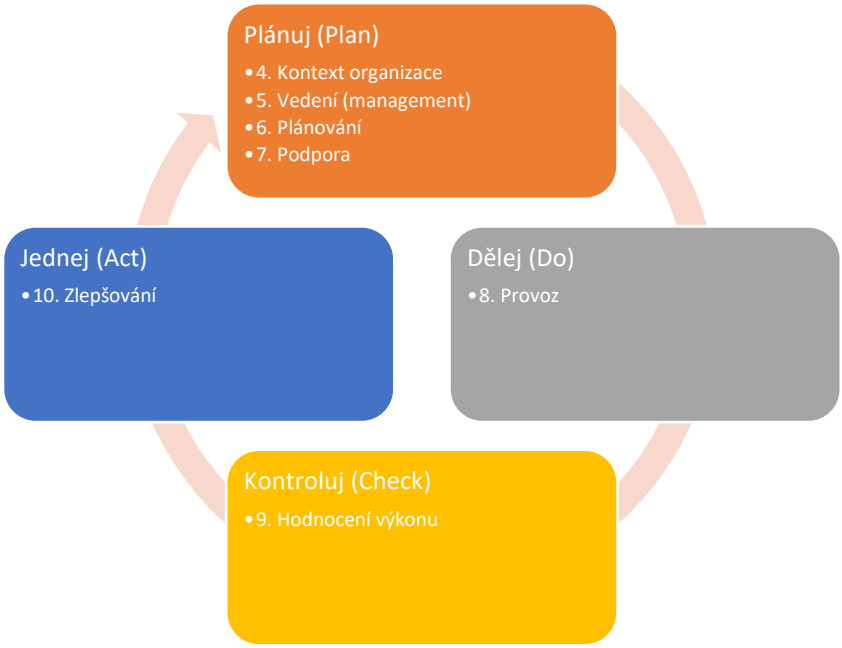
V normě je silně prosazován procesní přístup k řešení ISMS využívající Demingův model PDCA (odvozeno z prvních písmen slov *Plan – Do – Check – Act*, volně přeložitelné do češtiny jako *Plánuj – Dělej – Kontroluj – Jednej*). Cyklus PDCA může být aplikován na veškeré procesy ISMS tak, jak jsou definovány normou. Schéma na Obr. 2 ukazuje, které kapitoly normy odpovídají jednotlivým fázím cyklu PDCA.

Příloha A této normy vyjmenovává cíle opatření a jednotlivá opatření. Kapitola 9 této přílohy se zabývá Řízením přístupu, dále se dělí na 4 podkapitoly.

- Požadavky organizace na řízení přístupu
- Řízení přístupu uživatelů
- Odpovědnosti uživatelů
- Řízení přístupu k systémům a aplikacím

Kapitola 11 přílohy vyjmenovává opatření Fyzické bezpečnosti a bezpečnosti prostředí, které dělí do dvou podkapitol – Bezpečné oblasti (klade si za cíl předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení pro zpracování informací organizace) a Zařízení (cílem je předcházet ztrátě, poškození a krádeži nebo kompromitaci aktiv a přerušení činnosti organizace). (8)

Pro tuto práci bude tyto části přílohy A normy ČSN ISO/IEC 27001 stěžejní.



Obr. 2: Norma ISO/IEC 27001 v Demingově cyklu PDCA (8)

2.3.3 Norma ČSN ISO/IEC 27002

Aktuální verze ČSN ISO/IEC 27002:2014 nahrazuje v České republice normu ČSN ISO/IEC 17799:2006, je překladem normy ISO/IEC 27002:2013, která však nahrazovala ISO/IEC 27002:2005. Je určena pro organizace k použití jako doporučení pro výběr opatření v rámci procesu zavádění ISMS založeného na normě ISO/IEC 27001, nebo jako pokyny pro organizace implementující obecná opatření bezpečnosti informací. Pomáhá organizacím vybrat vhodná opatření v rámci procesu zavádění systému řízení bezpečnosti informací dle normy ISO/IEC 27001, zavést obecně uznávaná opatření bezpečnosti informací a vypracovat vlastní směrnice k řízení bezpečnosti informací. Obsahuje celkem 35 hlavních kategorií bezpečnosti a 114 kontrol. (14)

2.3.4 Norma ČSN ISO/IEC 27003

Účelem normy ISO/IEC 27003 je poskytnout praktická doporučení při vývoji plánu implementace pro systém řízení informací v organizaci v souladu s ISO/IEC 27001. Proces popsaný v této normě byl navržen tak, aby poskytoval podporu pro zavedení ISO/IEC 27001 a zdokumentoval přípravu zahájení plánu implementace ISMS v organizaci, definování organizační struktury pro projekt, získání souhlasu vedení, kritické činnosti pro projekt ISMS a příklady naplnění požadavků normy ISO/IEC 27001. Norma je určena pro organizace, které zavádějí ISMS a je aplikovatelná pro všechny typy

organizací všech velikostí. Norma ISO/IEC 27003 dává doporučení a vysvětlení, nespecifikuje žádné požadavky. (15)

Jelikož se jedná o normu z roku 2011, odkazuje se dnes již neplatnou na ISO/IEC 27001:2005 (ČSN ISO/IEC 27001:2006). Pro použití s aktuální ČSN ISO/IEC 27001:2014 je tedy nutné dbát jisté obezřetnosti.

2.3.5 Norma ČSN ISO/IEC 27004

Mezinárodní norma v aktuální verzi ČSN ISO/IEC 27004:2011 poskytuje doporučení pro vývoj a použití metrik a měření za účelem hodnocení účinnosti zavedeného systému řízení bezpečnosti informací (ISMS) a opatření nebo skupin opatření, jak je uvedeno v ISO/IEC 27001. Je aplikovatelná na všechny typy a velikosti organizací. Doporučení podporují proces revize, který napomáhá určit, zda některé procesy či opatření ISMS vyžadují změnu nebo zlepšení. (16)

I u této normy je nutná jistá obezřetnost při použití, neboť vzhledem ke svému roku vydání může odkazovat na dnes již neplatné normy, které byly nahrazeny novými verzemi, jako například ČSN ISO/IEC 17799:2006 nebo ISO/IEC 27000:2009 a další. (16)

2.3.6 Norma ČSN ISO/IEC 27005

Mezinárodní norma ČSN ISO/IEC 27005 v aktuální revizi z roku 2013 poskytuje doporučení pro řízení rizik bezpečnosti informací. Podporuje přitom obecný koncept specifikovaný v ISO/IEC 27001. Znalost konceptu, modelů, procesu a terminologie popsané v ISO/IEC 27001 a 27002 je důležitá pro pochopení této normy. Norma ISO/IEC 27005 je aplikovatelná na všechny typy organizací, které mají v úmyslu řídit rizika, která mohou narušit bezpečnost informací organizace. (2)

2.3.7 Norma ČSN ISO/IEC 27006

Mezinárodní norma ISO/IEC 27006 v české verzi z roku 2016 specifikuje požadavky a poskytuje doporučení pro orgány provádějící audit a certifikaci systému řízení bezpečnosti informací (ISMS) a doplňuje tak požadavky obsažené v ISO/IEC 17021-1 a také v ISO/IEC 27001. Norma je především určena k podpoře akreditace certifikačních orgánů poskytujících certifikace ISMS. Může být použita jako kriteriální dokument pro akreditaci, interní hodnocení nebo při jiných auditních procesech. (17)

2.3.8 Norma ISO/IEC TR 27019

Technická zpráva ISO/IEC TR 27019:2013 poskytuje hlavní zásady založené na ISO/IEC 27002:2005 aplikované na systémy řízení procesů používaných v energetickém průmyslu. Jejím úkolem je rozšířit řadu norem ISO/IEC 27000 na oblast řídicích systémů a automatizační techniky. To umožní energetickému průmyslu zavést standardizovaný systém řízení bezpečnosti informací v souladu s ISO/IEC 27001. Rozsah normy se vztahuje na systémy řízení procesů používaných pro monitorování a řízení výroby, přenosu, distribuce a skladování elektrické energie, tepla nebo plynu. (18) Jako jediná z dosud zmíněných norem nebyla tato prozatím přeložena do českého jazyka.

2.4 Předběžná norma ČSN P 73 4450-1

Předběžná norma ČSN P 73 4450-1 z roku 2013 stanovuje obecné požadavky na systém fyzické ochrany prvku kritické infrastruktury pro minimalizaci dopadů antropogenních hrozeb, včetně teroristického útoku. Je určena především pro subjekty kritické infrastruktury, orgány státní správy a samosprávy a poskytovatele bezpečnostních služeb. Ostatním uživatelům může sloužit jako metodický návod pro zajištění úrovně a rozsahu fyzické ochrany prvků kritické infrastruktury. (4)

Norma bezpečnostní opatření fyzické ochrany dělí na technická a režimová opatření a fyzickou ostrahu. Technická opatření, jimiž norma rozumí mechanické a elektronické prostředky, které mají za úkol chránit hranici areálu, plášť objektu a vnitřní prostory objektu, pak dále dělí na elektrickou požární signalizaci a systém technické ochrany, u kterých vyjmenovává jednotlivé prvky. Režimovými opatřeními se rozumí soubor interních závazných a přesně definovaných pokynů, příkazů omezení a postupů, zajišťují vzájemné vazby mezi bezpečnostními opatřeními a uživateli objektu. Norma vymezuje požadavky na osoby pověřené výkonem fyzické ostrahy a vyjmenovává činnosti, které by tyto osoby měly vykonávat. (4)

V závěrečných dvou kapitolách se nejprve zabývá požadavky na bezpečnostní opatření fyzické ochrany, a poté fázemi životního cyklu systému fyzické ochrany, tedy jeho návrhem, implementací a provozem. V příloze udává přehled stálých a doplňkových bezpečnostních opatření. (4)

Kat.	Bezp. zóna	Charakteristika objektu	Příklad
I.	Zvlášť zabezpečená	Objekt s kritickým významem pro prvek KI, nenahraditelný nebo obtížně nahraditelný	Dispečink, pracoviště ICT, serverovna
II.	Zabezpečená	Objekt se zásadním významem pro prvek KI	Klíčové zařízení výroby, administrativní budova sídla společnosti, telefonní ústředna, strojovna, archiv
III.	Chráněná	Objekt s důležitým významem pro zabezpečení funkčnosti prvku KI	Vybraný skladový prostor, generátorová stanice, vybraná opravárenská dílna
IV.	Kontrolovaná	Neprovozní a nevýrobní objekt, který nemá přímý vliv na bezpečnost	Garáž, dílna, odstavná plocha, školící budova

Tab. 2: Bezpečnostní kategorie objektů prvku KI a bezpečnostní zóny. Zdroj: (4)

2.4.1 Technická opatření – systém technické ochrany a požární signalizace

Systém technické ochrany (STO) je soubor prostředků vnitřní a vnější ochrany a tvoří systém, který zabraňuje, ztěžuje, detekuje nebo dokumentuje narušení fyzické ochrany. Dále budou vyjmenovány jednotlivé prvky. Systém technické ochrany musí být spravován vyškolenou osobou, jejíž znalosti jsou periodicky prověřovány. (4) Správou se rozumí:

- Pravidelná údržba (funkční zkoušky, prohlídky, revize)
- Součinnost s dodavateli údržby a servisu STO a jejich kontrola
- Plánování obnovy a rozvoje STO, řízení požadavků na údržbu
- Nakládání se záznamy CCTV
- Nakládání s provozní dokumentací
- Správa přístupových oprávnění
- Školení zaměstnanců a obsluhy STO
- Detekce závad STO a řešení jejich následků

Správu STO může zajišťovat vlastní zaměstnanec nebo externí subjekt na základě smlouvy. (4)

2.4.1.1 Mechanické zábranné prostředky

Mechanické zábranné prostředky slouží k zamezení přístupu nebo jeho ztížení, případně k odrazení náhodného pachatele před vniknutím do chráněného prostoru. Zároveň vytváří časovou prodlevu pro přijetí vhodných opatření proti narušiteli (zdržení narušitele). (4)

Jednotlivými prostředky jsou (příklady):

- Oplocení a ohrazení
- Dveře, brány, vrata, turnikety, okna, mříže, okenice
- Bezpečnostní skla a fólie
- Zámky a uzamykací systémy

Mechanické zábranné prostředky lze rozdělit i podle oblasti jejich využití:

- Perimetr areálu
    - Vnější oplocení
    - Vstupy (vstupní branka) a vjezdy (vjezdová a vlečková brána)
    - Budovy v perimetru
- Vnější prostory
    - Venkovní stanoviště silového energetického zařízení
    - Odstavné plochy uvnitř objektu s uloženým majetkem
    - Vstupy do průchozích kabelových kanálů
- Vnitřní prostory a budovy
    - Vstupní dveře a vrata v plášti budovy včetně nouzových východů a vstupů z kabelových kanálů
    - Uzamykací systém nebo visací zámek ve vstupních dveřích a vratech do budovy
    - Samouzavírací mechanismus na hlavních vstupních dveřích do budovy
    - Prosklené části v plášti budovy (dveře, okna)
    - Prosklené části v plášti budovy pod úrovní okolního terénu (sklepní okna)
    - Další technické otvory v plášti budovy
    - Pevné žebříky na plášti budovy ústící na střechu

2.4.1.2 Poplachový zabezpečovací a tísňový systém (PZTS)

Poplachový zabezpečovací systém slouží k včasnému zjišťování, indikace a vyhodnocování neoprávněného vniknutí či napadení osob, vyrozumění zásahových skupin a fyzické ostrahy a aktivaci dalších bezpečnostních opatření. Mimo to může sloužit rovněž jako kontrola dodržování režimových opatření. (4)

- Ochraně perimetru, prostoru a pláště budovy
- Ochrana technických a technologických zařízení
- Tísňové systémy

2.4.1.3 CCTV sledovací systémy

CCTV systémy se používají pro sledování, přenos, zobrazování a dokumentace pohybu osob a dopravních prostředků. Poskytují rychlé a spolehlivé obrazové informace pro zabezpečovací, bezpečností a monitorovací činnost, jejich záznam lze zpětně vyhodnocovat. Umožňují dálkový dohled v případě nepřítomnosti osob v objektu. (4)

- Pevné a otočné kamery
- Speciální kamery (např. termovizní)

2.4.1.4 Systémy kontroly vstupu (SKV)

Systém kontroly vstupu zajišťuje režim vstupu osob a vjezdu dopravních prostředků do chráněných prostorů, lze pomocí něho kontrolovat a dokumentovat pohyb v chráněných prostorech podle nastavených oprávnění, a tedy i identifikovat pokusy o neoprávněný přístup do chráněných prostor. (4) Systém kontroly vstupu může používat následující prostředky (mimo jiné):

- Čipy
- Identifikační karty
- Biometrické snímače

2.4.1.5 Systémy přivolání pomoci

Systém přivolání pomoci aktivuje poplach přenesením signálu na centrální pult bezpečnostní služby, vyrozumí fyzickou ostrahu a případné další zásahové skupiny. (4) Tvoří ho následující prostředky:

- Aktivační zařízení

- Poplachový přenosový systém
- Poplachové přijímací centrum/pult centrální ochrany

2.4.1.6 Poplachové přenosové systémy a zařízení (PPSZ)

Poplachové přenosové systémy pomocí přenosových prostředků přenáší informace ze zabezpečovacích zařízení. (4)

2.4.1.7 Kombinované a integrované systémy

Kombinované a integrované systémy automatizují vzájemné vazby jednotlivých systémů, čímž zjednodušují jejich obsluhu. Vzájemně integrované systémy si mezi sebou mohou vyměňovat data, sdílet některá zařízení, vybavení a přenosové trasy. Mohou být schopny poskytovat doplňkové informace (obrazem, textem nebo zvukem). (4)

2.4.1.8 Přístroje pro použití ve dveřních vstupních audiosystémech a videosystémech

Umožňují navázání komunikace mezi osobou požadující vstup a osobou povolující vstup. Ověření identity provádí osoba povolující vstup na základě zvuku nebo obrazu. Po úspěšné identifikaci může osoba povolující vstup dálkově odblokovat dveře. (4)

2.4.1.9 Dohledová a poplachová přijímací centra (DPPC)

Dohledová centra vykonávají nepřetržitý dohled nad připojenými poplachovými systémy. Včas zjišťují, indikují a vyhodnocují všechny poplachové a případně i poruchové signály. Závisí na nich rychlost a efektivnost zákroku zásahových skupin a fyzické ostrahy. (4)

2.4.1.10 Nouzové zvukové systémy a hlasová výstražná zařízení

Nouzové zvukové systémy mají za cíl vysílání informací a případně řízení evakuace. Používají se systémy s tónovými signály (např. siréna, klakson) a systémy s hlasovým hlášením (např. obecní rozhlas). (4)

2.4.1.11 Bezpečnostní a nouzové osvětlení

Bezpečnostní a nouzové osvětlení si klade za cíl odrazení náhodného pachatele před vniknutím do chráněného prostoru, případně jeho snadnější identifikaci. (4)

Příklad technických prostředků:

- Trvalé osvětlení za snížené viditelnosti
- Osvětlení při detekci pohybu

- IR osvětlení

2.4.1.12 Elektrická požární signalizace (EPS)

Požární signalizace je často součástí kombinovaných a integrovaných systémů. Instaluje se v souladu s požadavky danými příslušnými právními předpisy (Zákon č. 133/1985 Sb. o požární ochraně, Vyhláška č. 246/2001 Sb. o požární prevenci a Vyhláška č. 23/2008 Sb. o technických podmínkách požární ochrany). EPS musí být instalována u prvku KI v objektech bezpečnostní kategorie I. (viz Tab. 2), doporučuje se instalace i v dalších důležitých objektech. V objektech prvku KI, kde není vyžadována instalace EPS, lze zajistit signalizaci vzniku požáru čidly zapojenými do PZTS. (4)

2.4.1.13 Oblasti využití PZTS, CCTV, SKV a PPSZ

- Perimetr areálu
    - Vnější oplocení
    - Vstupy (vstupní branka) a vjezdy (vjezdová a vlečková brána)
    - Budovy v perimetru
    - Ostatní prostupy
- Vnější prostory
    - Venkovní stanoviště silového energetického zařízení
    - Odstavné plochy uvnitř objektu s uloženým majetkem
    - Vstupy do průchozích kabelových kanálů
    - Evidence vstupu ve venkovních prostorách objektu
    - Přenos poplachových a jiných funkčních stavů PZS na energetický dispečink nebo regionální dohledové pracoviště
- Vnitřní prostory a budovy
    - Vstupní dveře a vrata v plášti budovy včetně nouzových východů a vstupů z kabelových kanálů
    - Prosklené části v plášti budovy (dveře, okna) přístupné i nepřístupné z dosažitelných míst (římsy, střechy, žebříky, balkony)
    - Prosklené části v plášti budovy pod úrovní okolního terénu (sklepní okna)
    - Další technické otvory v plášti budovy
    - Pevné žebříky na plášti budovy ústící na střechu
    - Vyústění kabelového kanálu

- Vstupní dveře a celé prostory související s provozem objektu
- Vnitřní prostory u vstupních dveří do budovy a další společné prostory
- Prostor s instalovanou ústřednou PZTS
- Evidence vstupu do budovy a vybraných prostor souvisejících s provozem objektu (v PZTS nebo SKV)
- Přenos poplachových a jiných funkčních stavů PZS na energetický dispečink nebo regionální dohledové pracoviště

2.4.2 Režimová opatření

Režimová opatření zajišťují vzájemné vazby mezi bezpečnostními opatřeními a uživateli objektu. (4) Týkají se:

- Činnosti pracovníků uvnitř organizace
- Pohybu a chování externích osob (návštěvy, dodavatelé)
- Oběhu dokladů a informací uvnitř organizace (spisový řád)
- Vstupu a výstupu informací, dat a dokumentů vně podniku

Mezi režimová opatření patří zejména:

- Režim vstupu/výstupu osob (zaměstnanci, návštěvy, dodavatelé a další)
- Režim vjezdu/výjezdu vozidel
- Režim pohybu osob a vozidel v objektu
- Režim pohybu majetku (hmotného i nehmotného)
- Režim nakládání s identifikačními prvky (klíče, kódy, karty)
- Režim obsluhy systému technických opatření (STO)
- Opatření a postupy pro mimořádné situace

2.4.3 Fyzická ostraha

Fyzická ostraha může být zajištěna vlastními zaměstnanci subjektu KI nebo smluvním poskytovatelem bezpečnostních služeb. Osoba vykonávající fyzickou ostrahu musí splňovat podmínky odborné způsobilosti k výkonu strážní služby dle Živnostenského zákona (č. 455/1991 Sb.). (4)

Základní formy výkonu fyzické ostrahy pro účel ochrany prvku KI:

- Místní výkon na pevných stanovištích nebo obchůzka (pohyblivé stanoviště)

- Mobilní hlídka
- Dálkový dohled prostřednictvím DPPC

Pracovníci ostrahy vykonávají zejména tyto činnosti:

- Kontrola vstupu/výstupu osob
- Kontrola vjezdu/výjezdu vozidel
- Kontrola pohybu materiálu z/do objektu
- Správa klíčů (výdej, vracení, evidence)
- Informační služba
- Kontrolní obchůzková činnost ve stanovených periodách po stanovených trasách
- Identifikace mimořádných situací
- Provádění zákroku v případě ohrožení života, zdraví nebo majetku
- Provádění ohlašovací povinnosti v případě ohrožení života, zdraví nebo majetku
- Součinnost se složkami IZS

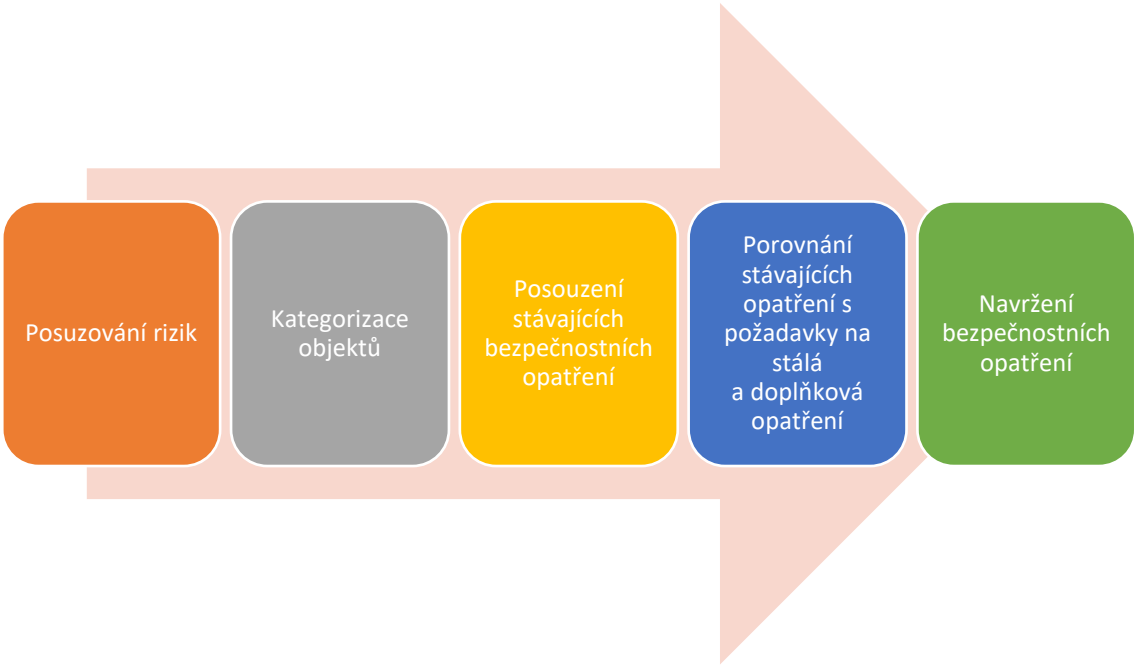
2.4.4 Systém fyzické ochrany

Sedmá kapitola normy ČSN P 73 4450-1 se zabývá životním cyklem systému fyzické ochrany znázorněný na Obr. 3. Nejprve se věnuje jeho návrhu, který dále dělí na fáze:

- Posuzování rizik
- Kategorizace objektů (viz Tab. 2)
- Posouzení stávajících bezpečnostních opatření fyzické ochrany
    - Analýza bezpečnostní dokumentace
    - Bezpečnostní prohlídka
- Porovnání stávajících bezpečnostních opatření fyzické ochrany s požadavky na stálá a doplňková bezpečnostní opatření
- Navržení bezpečnostních opatření fyzické ochrany

Poté se věnuje implementaci systému, kdy říká, že nejprve musí být implementována opatření pro kategorii I, nejpozději pro kategorii IV v kontrolované zóně podle Tab. 2. V závěru se zabývá provozem systému fyzické ochrany. Klade požadavky na pracovníky a ověřování funkčnosti bezpečnostních opatření fyzické kontroly. Vyjmenovává jednotlivé nástroje pro ověření (kontroly, audity, penetrační testy, analýzu rizik, simulaci mimořádných situací) a stanovuje, že v případě implementace nových nebo stávajících

bezpečnostních opatření FO musí být v nezbytném rozsahu upravena související bezpečnostní dokumentace. (4)



Obr. 3: Proces navržení systému fyzické ochrany. Zdroj: Vlastní dle ČSN P 73 4450-1 (4)

2.5 Zákony a vyhlášky

Společnost, pro niž je tato diplomová práce zpracována, se zabývá distribucí a prodejem elektrické energie a zemního plynu v některých krajích České republiky (podrobnější představení společnosti se nachází dále v kapitole 3.1), z toho důvodu se musí řídit zákony a nařízeními specifickými pro tento obor podnikání. Tato podkapitola zmiňuje některé z těchto zákonů, které svým obsahem mohou nějak ovlivnit *Návrh přístupového systému jako součást řešení fyzické bezpečnosti* pro danou energetickou společnost.

2.5.1 Krizový zákon č. 240/2000 Sb.

Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon) stanovuje působnost a pravomoc státních orgánů a orgánů samosprávy a práva a povinnosti fyzických i právnických osob při přípravě na kritické situace, jejich řešení a při ochraně kritické infrastruktury. Vymezuje povinnosti subjektů kritické infrastruktury jakožto správce kritické infrastruktury. Určuje i odpovědnost za porušení těchto povinností. (7)

2.5.2 Nařízení vlády č. 432/2010 Sb.

Nařízení vlády č. 432/2010 o kritériích pro určení prvku kritické infrastruktury definuje odvětvová a průřezová kritéria pro určení prvku kritické infrastruktury dle zákona č. 240/2000 Sb. Průřezová kritéria hodnotí kritičnost prvku podle počtu zasažených osob (více než 250 usmrceno či více než 2500 zraněno s nutnou hospitalizací, nebo vážně zasažený každodenní život více než 125 000 osob) nebo ekonomiky (ztráta více než 0,5 % hrubého domácího produktu).

Odvětvová kritéria vyjmenovávají konkrétní případy v daných odvětvích. V elektroenergetice se jedná o výrobny elektrické energie s výkonem vyšším než daná mez, o přenosovou soustavu a část distribuční soustavy. Zde se jedná o elektrické stanice o napětí 110 kV, případně další stanice (110/10 kV, 110/22 kV a 110/35 kV) určené podle strategického významu a technický dispečink provozovatele distribuční soustavy. Odvětvová kritéria se zabývají i ostatními oblastmi energetiky (plyn, teplo, ropa), vodním hospodářstvím, komunikačními a informačními systémy, zemědělstvím, zdravotnictvím a dalšími obory. (19)

2.5.3 Kybernetický zákon č. 181/2014 Sb.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) vstoupil v platnost na začátku roku 2015 a upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Nevztahuje se na informační a komunikační systémy nakládající s utajovanými informacemi.

V první části zákona jsou vymezeny některé pojmy, druhá hlava nese název *Systém zajištění kybernetické bezpečnosti*. V té definuje pojem bezpečnostní opatření a dále ho dělí na organizační a technická opatření, u kterých vyjmenovává jednotlivé příklady (organizační opatření: ISMS, řízení rizik, bezpečnostní politika, bezpečnost lidských zdrojů, …; technická opatření: fyzická bezpečnost, nástroj pro ověřování identity uživatelů, nástroj pro řízení přístupových oprávnění, aplikační bezpečnost, kryptografické prostředky a další). Dále definuje kybernetickou bezpečnostní událost (taková událost, která může způsobit narušení bezpečnosti informací) a incident (narušení bezpečnosti informací v důsledku události), určuje orgány a osoby, které jsou povinny kybernetické incidenty hlásit a evidovat.

V paragrafu 11 zavádí pojem opatření a dělí jej na 3 druhy: varování, reaktivní opatření a ochranné opatření. Varování vydává zákonem určený úřad (Národní bezpečnostní úřad – NBÚ). Úřad vydává rozhodnutí, v němž uloží provedení reaktivního opatření. Osoby, jimž to bylo nařízeno, jsou povinny opatření provést a oznámit úřadu jeho výsledek. Ochranné opatření úřad ukládá za účelem preventivního zvýšení ochrany informačních služeb nebo systémů na základě již vyřešeného kybernetického incidentu.

Dále zákon vymezuje působnost národního CERT, který působí jako kontaktní místo, přijímá hlášení o kybernetických bezpečnostních incidentech, vyhodnocuje je a poskytuje metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu a dále předává Úřadu údaje o kybernetických bezpečnostních incidentech bez uvedení ohlašovatele kybernetického bezpečnostního incidentu.

Třetí hlava (§21) uvádí, že stavem kybernetického nebezpečí se označuje situace, kdy je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, čímž by mohlo dojít nebo již došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací. O vyhlášení takového stavu rozhoduje ředitel Úřadu na dobu nezbytně nutnou, nejdéle však 7 dnů, kterou lze opakovaně prodloužit až na 30 dnů.

Čtvrtá hlava zákona přiděluje Úřadu výkon státní správy v oblasti kybernetické bezpečnosti a stanovuje jeho práva a povinnosti v této oblasti. V páté hlavě zákona je zaneseno, že Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti, tedy zda dotčené orgány a osoby plní povinnosti stanovené tímto zákonem. V případě zjištění nedostatků uloží danému orgánu či osobě, aby je ve stanovené lhůtě (stanoveným způsobem) odstranila. Pokud osoba nesplní povinnost uloženou Úřadem, dopustí se správního deliktu, za což může být uložena pokuta ve výši až 100 000 Kč.

V samotném závěru zákon pomocí přechodných ustanovení určuje, kdy mají být splněny které požadavky dané tímto zákonem. Také ukládá Úřadu vyhláškou stanovit mimo jiné strukturu a obsah bezpečnostní dokumentace. (5)

2.5.4 Nařízení vlády č. 315/2014 Sb.

Nařízení vlády č. 315/2014 o kritériích pro určení prvku kritické infrastruktury aktualizuje původní Nařízení vlády č. 432/2010 Sb. Zavádí nové znění přílohy s názvem

„Odvětvová kritéria pro určení prvku kritické infrastruktury“, do které oproti původní verzi především přidává v kapitole *VI. Komunikační a informační systémy* nový bod *G. Oblast kybernetické bezpečnosti*. Mimo to ještě mírně mění či zpřesňuje některé další body. (19) (6)

2.5.5 Vyhláška č. 316/2014 Sb.

Vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) k provedení některých paragrafů zákona č. 181/2014 Sb. (kybernetického zákona). *„Vyhláškou se stanoví obsah a struktura bezpečnostní dokumentace pro informační systém kritické informační infrastruktury (KII), komunikační systém kritické infrastruktury (KI) nebo významný informační systém, obsah bezpečnostních opatření, rozsah jejich zavedení, typy a kategorie kybernetických bezpečnostních incidentů a způsob hlášení kybernetického bezpečnostního incidentu, náležitosti oznámení o provedení reaktivního opatření a jeho výsledku a vzor kontaktních údajů a jeho formu.“* (20)

Jednotlivé paragrafy vyhlášky nejprve rozebírají organizační opatření – Systém řízení bezpečnosti informací (§3), řízení rizik (§4), bezpečnostní politika (§5), organizační bezpečnost (§6), stanovení bezpečnostních požadavků pro dodavatele (§7), řízení aktiv (§8), bezpečnost lidských zdrojů (§9), řízení provozu a komunikací (§10), řízení přístupu a bezpečné chování uživatelů (§11), akvizice, vývoj a údržba (§12), zvládání kybernetických bezpečnostních událostí a incidentů (§13), řízení kontinuity činností (§14), kontrola a audit kritické informační infrastruktury a významných informačních systémů (§15).

V druhé hlavě vyhláška zmiňuje technická opatření – Fyzická bezpečnost (§16), nástroj na ochranu integrity komunikačních sítí (§17), nástroj pro ověřování identity uživatelů (§18 – stanovuje mimo jiné i minimální požadavky na délku a složitost hesla), nástroj pro řízení přístupových oprávnění (§19), nástroj pro ochranu před škodlivým kódem (§20), nástroj pro zaznamenávání činnosti KII a VIS, jejich uživatelů a administrátorů (§21), nástroj pro detekci kybernetických bezpečnostních událostí (§22), nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí (§23), aplikační bezpečnost

(§24), kryptografické prostředky (§25), nástroj pro zajišťování úrovně dostupnosti (§26) a bezpečnost průmyslových a řídicích systémů (§27).

V třetí hlavě vyhláška stanovuje požadavky na obsah, rozsah a formu bezpečností dokumentace, kterou musí osoba nebo orgán dle kybernetického zákona vést a aktualizovat. Dále říká, že orgán nebo osoba, jejíž informační systém KII, komunikační systém KII nebo VIS je zcela zahrnut do systému řízení bezpečnosti informací (ISMS), který byl certifikován dle příslušné technické normy (explicitně uvedeno ISO/IEC 27001:2013, případně ČSN ISO/IEC 27001:2014) akreditovaným certifikačním orgánem a vede další dokumenty, splňuje požadavky na zavedení bezpečnostních opatření podle kybernetického zákona a této vyhlášky.

Dále vyhláška vyjmenovává typy a kategorie kybernetických bezpečnostních incidentů, předepisuje formu a náležitosti hlášení kybernetických bezpečnostních incidentů a stanovuje formu oznámení o provedení reaktivních opatření.

V přílohách vyhláška rozebírá hodnocení a úrovně důležitosti aktiv, hodnocení rizik, minimální požadavky na kryptografické algoritmy, strukturu bezpečnostní dokumentace a předkládá vzory některých formulářů. (20)

2.5.6 Vyhláška č. 317/2014 Sb.

Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích stanovuje významné informační systémy a jejich určující kritéria podle §6 písmene d) Kybernetického zákona (č. 181/2014 Sb.). Vyhláška ve své příloze vyjmenovává seznam významných informačních systémů a dále ukládá, že o příslušnosti mezi významné informační systémy u systémů neuvedených v tomto seznamu rozhoduje správce konkrétního informačního systému na základě určujících kritérií (*Oblastních určujících kritérií* nebo *Dopadových určujících kritérií*). Dle vyhlášky mají dopadová kritéria stanovenou dolní hranici, horní hranice je dána krizovým zákonem č. 240/2000 Sb. (při překročení horní hranice je systém zařazen jako prvek kritické infrastruktury, nikoli jako významný informační systém). (21)

2.5.7 Energetický zákon č. 458/2000 Sb.

Celým názvem „Zákon č. 458/2000 Sb. o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon)“ nabyl

účinnosti dne 1. ledna 2001. Energetický zákon upravuje podmínky podnikání a výkon státní správy v energetických odvětvích. Zákon definuje a vyjmenovává, co je podnikáním v energetických odvětvích, a že pro tato podnikání je nutná licence dle energetického zákona, definuje pojmy spojené s podnikáním v energetice (např. *přenosová soustava*, *odběrné místo* a další). Dále je v zákoně zakotvena činnost Energetického regulačního úřadu (ERÚ) se sídlem v Jihlavě a Operátora trhu (OTE, a.s.).

Ve zvláštní části se věnuje jednotlivým odvětvím energetiky – Elektroenergetika, plynárenství a teplárenství. V každé části určuje jednotlivé účastníky trhu, definuje vztahy mezi nimi a rovněž určuje jejich práva a povinnosti. Účastníky trhu s elektřinou jsou dle energetického zákona následující subjekty:

- výrobci elektřiny,
- provozovatel přenosové soustavy,
- provozovatelé distribučních soustav,
- operátor trhu,
- obchodníci s elektřinou,
- zákazníci (odběratelé).

Pro plynárenství uvádí podobné rozdělení, jen navíc přidává „provozovatele zásobníku plynu“. Teplárenství je pro tuto práci bezpředmětné.

Zákon dále přesně definuje ochranná pásma pro jednotlivá energetická zařízení. Nakonec vymezuje činnost Státní energetické inspekce a zabývá se ukládáním pokut. (3)

2.5.8 Zákon č. 101/2000 Sb.

Zákon č. 101/2000 Sb. Zákon o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000 upravuje práva a povinnosti při zpracování osobních údajů a stanoví podmínky, za nichž se uskutečňuje předání osobních údajů do jiných států. Zákon zřizuje Úřad pro ochranu osobních údajů (ÚOOÚ) a vymezuje jeho působnost

Zákon se vztahuje na osobní údaje, které zpracovávají státní orgány nebo jiné orgány veřejné moci, jakož i fyzické a právnické osoby. Vztahuje se na veškeré zpracování osobních údajů, ať k němu dochází automatizovaně nebo jinými prostředky. Nevztahuje se na zpracování osobních údajů, které provádí fyzická osoba pro osobní potřebu, stejně

jako se nevztahuje na nahodilé shromažďování osobních údajů, pokud nejsou dále nijak zpracovávány.

Osobním údajem se rozumí jakákoli informace týkající se určeného nebo určitelného subjektu osobních údajů. Subjektem údajů je fyzická osoba, k níž se osobní údaje vztahují. Citlivým údajem je osobní údaj vypovídající o národnostním, rasovém nebo etnickém původu, politických postojích, odsouzení za trestný čin, zdravotním stavu a sexuálním životě subjektů a genetický údaj subjektu údajů. Citlivým údajem je také biometrický údaj, který umožňuje přímou identifikaci nebo autentizaci subjektu údajů. Anonymním údajem je takový údaj, který nelze vztáhnout k určenému nebo určitelnému subjektu.

2.5.9 Obecné nařízení o ochraně osobních údajů (GDPR)

Celý název tohoto dokumentu zní *Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)*. Zkratka GDPR pochází z anglického *General Data Protection Regulation*. Toto nařízení vstoupí v účinnost 25. května 2018 a bude závazné pro všechny subjekty, které zpracovávají osobní údaje občanů EU (tedy i pro subjekty sídlící mimo EU). Nad rámec dosavadní úpravy mezi osobní údaje počítá i údaje technického rázu (IP adresa, cookies).

GDPR reguluje zacházení s jakýmikoli informacemi vztahujícími se k identifikované nebo identifikovatelné osobě. Pro zpracovatele a správce údajů stanovuje povinnosti (mimo jiné neprodleně hlásit jakékoli incidenty v oblasti osobních dat a jejich ochrany), definuje podmínky, za kterých mohou být osobní údaje zpracovávány, a dává subjektům těchto informací množství práv, včetně práva „být zapomenut“.

V České republice byl dosud podle zákona č. 101/2000 Sb. o ochraně osobních údajů hlavním regulátorem Úřad pro ochranu osobních údajů (ÚOOÚ) (22), který by měl v této funkci zůstat i po zavedení nařízení GDPR.

Nová práva občana po zavedení GDPR (výběr):

- Právo na přístup k datům, které o občanovi správce zpracovává.
- Právo na opravu dat, pokud občan zjistí, že jsou nesprávná.

- Právo na výmaz dat bez zbytečného odkladu.
- Právo být zapomenut.
- Právo na přenositelnost dat (ve strojově čitelném strukturovaném formátu).

Nové povinnosti institucí a firem po zavedení GDPR (výběr):

- Implementace záměrné a nezbytné ochrany dat.
- Jmenování pověřence pro ochranu osobních údajů (Data Protection Officer).
- Zavedení pseudoanonymizace osobních údajů.

V případě porušení, nezavedení či nepřipravenosti na nové nařízení hrozí povinným subjektům pokuty (vysoké až likvidační). Zatímco stávající zákon o ochraně osobních údajů stanovuje sankci za správní delikt v maximální výši 10 000 000 Kč. GDPR zavádí pokuty až do výše 20 000 000 € nebo do 4 % celosvětového objemu tržeb – jako horní hranice se bere vyšší z těchto dvou částek. (23)

2.6 Řízení rizik

Řízením rizik se blíže zabývá norma ČSN ISO/IEC 27005:2013. Ta proces řízení rizik definuje následovně:

1) Stanovení kontextu
2) Hodnocení rizik
    a. Identifikace rizik
    b. Analýza rizik
    c. Vyhodnocení rizik
3) Ošetření rizik
4) Akceptace rizik

Po celou dobu probíhá zároveň se všemi fázemi procesu ještě *komunikace rizik* a *monitorování a přezkoumávání rizik*. (2)

Pro správné ohodnocení rizik je nejprve nutné identifikovat a ohodnotit aktiva, k nimž se mohou možná rizika vztahovat.

2.6.1 Identifikace aktiv

Úkolem tohoto kroku je zjistit, jaká všechna aktiva společnost vlastní a v dalším kroku stanovit jejich hodnotu. Aktivem je jakýkoli movitý i nemovitý, hmotný i nehmotný. Aktivem jsou i znalosti, postupy, procesy, dokonce i zaměstnanci.

Norma ČSN ISO/IEC 27005:2013 doslova říká, že *„Aktivum je cokoli, co má pro organizaci ochranu a co tedy vyžaduje ochranu. […] Identifikace aktiv by měla být provedena na vhodném stupni podrobnosti, který poskytuje pro posouzení rizik dostatek informací. […] U každého aktiva by měl být identifikován vlastník aktiva k zajištění záruky a odpovědnosti za aktivum. Vlastník aktiva k němu možná nemá vlastnická práva, ale má přiměřenou odpovědnost za jeho produkci, vývoj, údržbu, používání a bezpečnost. Vlastník aktiva je nejvhodnější osobou pro určení hodnoty aktiva pro organizaci.“* (2)

Výstupem by měl být seznam aktiv, u nichž je třeba zajistit řízení rizik, a seznam procesů vztažených k aktivům a jejich důležitost. (2)

2.6.2 Hodnocení a úrovně důležitosti aktiv

V momentě, kdy známe, jaká aktiva v organizaci jsou, přistoupíme k jejich ohodnocení. Nejjednodušším způsobem ocenění aktiv by mohla být jejich pořizovací cena. Tu však nelze exaktně určit u všech možných aktiv, zejména těch nehmotných.

Nařízení vlády č. 316/2014 Sb. uvádí 3 stupnice o 4 úrovních (nízká, střední, vysoká, kritická) pro hodnocení důležitosti aktiv. První pro hodnocení důvěrnosti, druhou pro hodnocení integrity a třetí pro hodnocení dostupnosti. Jedná se o kvalitativní, nikoli kvantitativní hodnocení rizika. (20)

Další možností je stanovení bodové stupnice pro hodnocení aktiva pro proces analýzy rizik, která má semikvantitativní charakter. Bodová hodnota pro vyjádření důležitosti aktiva:

0) Žádná nebo nehodnocena
1) Nízká
2) Málo významná
3) Střední
4) Vysoká
5) Velmi vysoká

Pokud hodnotíme důležitost aktiva z více hledisek, můžeme výslednou hodnotu aktiva spočítat například jako vážený průměr jednotlivých hodnot.

2.6.3 Identifikace hrozeb

„Hrozba má potenciál poškodit aktiva a tím i samotnou organizaci. Hrozby mohou být přírodního nebo lidského původu, mohou být náhodné nebo úmyslné. Měly by být identifikovány zdroje všech hrozeb, jak náhodných, tak i úmyslných. Hrozba může vyvstat zevnitř i zvenčí organizace. Hrozby by se měly identifikovat podle typu (např. neoprávněné akce, fyzické zničení, technické poruchy) a pak, v případě potřeby, by se měly v rámci obecné třídy identifikovat jednotlivé hrozby. Tím se žádná hrozba neopomene a zároveň je omezen objem požadované práce. Některé hrozby mohou postihnout více než jedno aktivum. […] Při řešení hrozeb je zapotřebí brát v úvahu i aspekty životního prostředí a kultury.

Při aktuálním posouzení by se mělo přihlížet i k vnitřním zkušenostem z incidentů a minulým posouzením hrozeb. Tam, kde je to důležité, je možné nahlédnout i do jiných katalogů hrozeb za účelem doplnění seznamu obecných hrozeb. Katalogy hrozeb a statistiky jsou k dispozici u průmyslových orgánů, národních vlád, právních orgánů, pojišťoven atd.“ (2)

Výstupem by měl být seznam hrozeb s identifikací typu a zdroje hrozby.

2.6.4 Identifikace zranitelností

Cílem tohoto kroku je identifikovat zranitelnosti, které mohou být zneužity hrozbami, a tím mohou být poškozena aktiva nebo organizace.

Zranitelnosti lze identifikovat v následujících oblastech:

- Organizace,
- procesy a postupy,
- pracovníci,
- fyzické prostředí,
- konfigurace informačního systému,
- hardware, software a komunikační zařízení,
- závislost na externích stranách.

Samotná existence zranitelnosti sama o sobě škodu nepůsobí, musí existovat hrozba, která ji využije. Zranitelnost nemající odpovídající hrozbu nemusí vyžadovat opatření, ale měla by být rozpoznána a monitorována. Nesprávně přijaté nebo nefunkční opatření může představovat další zranitelnost. Zranitelnosti mohou souviset s vlastnostmi aktiva, které lze použít pro jiným způsobem nebo za jiným účelem, než bylo původně zamýšleno.

Výstupem je seznam zranitelností ve vztahu k aktivům, hrozbám a stávajícím opatřením. (2)

2.6.5 Identifikace následků

V tomto kroku by měly být identifikovány následky, které mohou pro aktivum znamenat ztrátu důvěrnosti, integrity a dostupnosti. Následkem může být ztráta účinnosti, nepříznivé provozní podmínky, ztráta obchodu, pověsti, škoda atd.

Tato činnost identifikuje škody nebo dopady na organizaci, jež by mohly být způsobeny podle scénáře incidentu. Scénář incidentu je popis hrozby zneužívající určitou zranitelnost nebo několik zranitelností. Je nutno určit následek incidentu a posuzovat přitom kritéria dopadu. Následek může ovlivnit jedno nebo více aktiv, případně jen část aktiva. Aktiva mohou mít stanovené hodnoty podle svých finančních nákladů nebo podle velikosti následků, jsou-li poškozena. Následky mohou být dočasného (např. výpadek) nebo trvalého charakteru (zničení aktiva).

Organizace by měly identifikovat následky scénářů incidentů mimo jiné z hlediska:

- vyšetřování a doby nápravy,
- ztráty času (pracovní/provozní doby),
- ztráty příležitosti,
- zdraví a bezpečnosti,
- finančních nákladů pro nápravu škody,
- pověsti a důvěryhodnosti.

Výstupem tohoto kroku je seznam scénářů incidentů s jejich následky vztahujícími se k aktivům nebo procesům. (2)

2.6.6 Analýza rizik

Analýzu rizik lze provádět v různých stupních podrobnosti v závislosti na kritičnosti aktiv, rozsahu známě zranitelnosti a předcházejících incidentech zasahujících organizaci. Může být kvalitativní nebo kvantitativní nebo kombinací obou. V praxi se nejprve pro získání obecné indikace úrovně rizika a odhalení větších rizik použije kvalitativní analýza, později může být nutné provést více konkrétní nebo kvantitativní analýzu, jejíž provedení je nákladnější a náročnější. (2)

2.6.6.1 Metody analýzy rizik

Kvalitativní analýza rizik používá k popisu velikost potenciálních následků (nízká, střední, vysoká) a pravděpodobnost, že se tyto následky vyskytnou. Její nevýhodou je závislost na subjektivním výběru škály klasifikačních atributů. Tyto školy lze upravit nebo přizpůsobit, aby odpovídaly okolnostem, a pro různá rizika lze použít různé popisy. Kvalitativní analýza by měla vycházet ze skutečných informací a dat, která jsou k dispozici. (2)

Kvantitativní analýza rizik používá stupnici s číselnými hodnotami, jak pro následky, tak i pro pravděpodobnost výskytu a využívá přitom informace z různých zdrojů. Kvalita analýzy závisí na přesnosti a úplnosti číselných hodnot a platnosti použitých modelů. Kvantitativní analýza rizik v mnoha případech používá historická data incidentů. Nevýhodou je nedostatek takových dat u nových rizik nebo slabých míst v bezpečnosti. Způsob, jimiž jsou následky a pravděpodobnost vyjádřeny, a způsoby, jimiž jsou kombinovány pro poskytnutí úrovně rizika, se mohou měnit podle typu rizika a čelu, pro který má být výstup posouzení rizik použit. (2)

2.6.6.2 Posouzení následků

Hodnotí se obchodní dopad na organizaci, který by mohl vyplývat z možných nebo skutečných incidentů bezpečnosti informací, s přihlédnutím k následkům porušení bezpečnosti informací, jako je ztráta důvěrnosti, integrity nebo dostupnosti aktiv.

Hodnotu dopadu na organizaci lze vyjádřit v kvalitativní i kvantitativní rovině, ale kterákoli metoda určující konkrétní peněžní hodnotu může obecně poskytovat více informací pro přijetí rozhodnutí a umožnit účinnější rozhodovací proces.

Hodnocení aktiv se určuje za použití následujících dvou kritérií:

- Hodnoty za náhradu aktiva,
- obchodní následky ztráty nebo kompromitace aktiva.

Toto hodnocení lze určit z analýzy dopadů na činnost organizace, kdy je tato hodnota obvykle vyšší než náklady na jednoduchou výměnu, v závislosti na důležitosti aktiva pro plnění cílů organizace. Hodnocení aktiva je klíčovým faktorem při posouzení dopadu scénáře incidentu. Následky nebo dopady na činnosti organizace lze určit modelováním výstupů události nebo souboru událostí, nebo extrapolací z experimentálních studií nebo minulých dat.

Následky lze vyjádřit na základě peněžních, technických, lidských nebo jiných pro organizaci vhodných kritérií. Finanční následky by měly být měřeny stejným přístupem, který byl použit pro pravděpodobnost hrozeb a zranitelnost. Důslednost v kvantitativním nebo kvalitativním přístupu je nutná.

Výstupem je seznam hodnocených následků scénáře incidentu vyjádřených s ohledem na aktiva a kritéria dopadu. (2)

2.6.6.3 Určení pravděpodobnosti incidentu

Při určování pravděpodobnosti každého scénáře a výskytu dopadu je nutné zohlednit, jak často se tyto hrozby vyskytují a jak snadno lze využít zranitelnosti. Je nutné brát v úvahu:

- Zkušenosti a platné statistiky o pravděpodobnosti hrozeb.
- U zdrojů úmyslných hrozeb motivaci a schopnosti a zdroje přístupné případným útočníkům, jakož i vnímání atraktivity a zranitelnosti aktiv pro případného útočníka
- U zdrojů náhodných hrozeb geografické faktory, možnost extrémních atmosférických podmínek a faktory s možným vlivem na lidská selhání nebo funkční poruchy zařízení.
- Zranitelnosti, jak jednotlivě, tak v souvislostech.
- Existující opatření a jejich účinnost na snížení zranitelnosti.

V závislosti na požadované přesnosti lze aktiva spojovat do skupin nebo je naopak rozdělit na jejich prvky a přiřadit scénáře k daným prvkům. Napříč geografickými lokalitami se může charakter hrozeb pro stejný typ aktiv měnit, nebo se může lišit účinnost existujícího opatření.

Výstupem je pravděpodobnost scénáře incidentů (kvalitativní nebo kvantitativní). (2)

2.6.6.4 Určení úrovně rizik

Na závěr analýzy je nutné určit úroveň rizik u všech důležitých scénářů incidentů. Analýza rizik přiřazuje kvalitativní nebo kvantitativní hodnoty k pravděpodobnosti a následkům rizika. Kromě toho může brát v úvahu poměr přínosů a nákladů, zájmy zainteresovaných stran a jiné proměnné vhodné pro hodnocení rizik. Odhadnuté riziko je kombinací (součinem) pravděpodobnosti a scénáře incidentu a jeho následků. Výstupem je seznam rizik s přiřazenými úrovněmi hodnot. (2)

2.6.7 Hodnocení rizik

Úroveň rizik vzešlá z analýzy rizik se porovná s kritérii hodnocení rizik a kritérii akceptace rizik. Rozhodnutí učiněná v rámci činnosti hodnocení rizik jsou založena zejména na akceptovatelné úrovni rizik. Při identifikaci rizik a v analýze by však měly být brány v úvahu rovněž následky, pravděpodobnost a stupeň důvěrnosti. Nahromadění většího množství nízkých nebo středních rizik může vyústit v daleko vyšší celková rizika a potřebu tuto situaci řešit.

Úvahy by měly zahrnovat:

- Vlastnosti bezpečnosti informací (aktiv): jestliže jedno kritérium není pro organizaci důležité, pak všechna rizika dopadající na toto kritérium nemusí být důležitá.
- Důležitost procesu nebo činnosti podporovaných určitým aktivem nebo souborem aktiv: jestliže má proces malou důležitost, rizikům s ním spojeným by měla být věnována menší pozornost, než rizikům potenciálně dopadajícím na důležitější procesy nebo činnosti.

Informací získaných o riziku v průběhu analýzy se využije k rozhodnutí o budoucích krocích. Rozhodnutí by měla zahrnovat skutečnost, zda by měla činnost být prováděna, a priority pro ošetření rizik s přihlédnutím k jejich odhadnutým úrovním.

Výstupem je seznam rizik, kterým byla udělena priorita podle kritérií hodnocení rizik v souvislosti se scénáři incidentů, jež k těmto rizikům vedou. (2)

2.6.8 Ošetření rizik

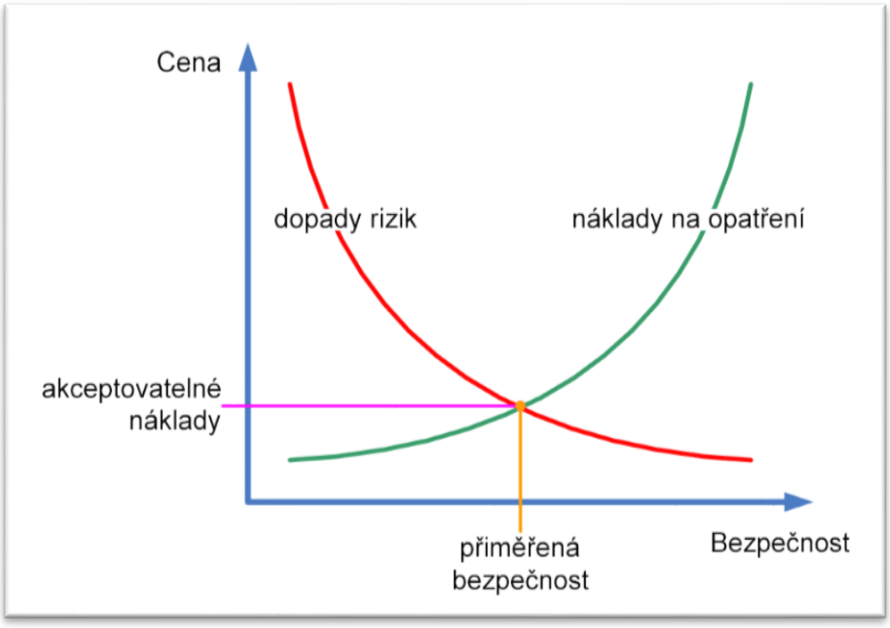
Vstupem procesu ošetření rizik je seznam rizik, jimž byla udělena priorita podle kritérií hodnocení rizik v souvislosti se scénáři incidentů, jež k těmto rizikům vedou. K dispozici jsou 4 volby ošetření rizik: modifikace, podstoupení, vyhnutí se a sdílení rizik. Způsob ošetření jednotlivých rizik by se měl vybírat na základě výstupu z posouzení rizik, očekávaných nákladů na implementaci a očekávaných přínosech plynoucích z těchto způsobů. Nepříznivé následky rizik by měly sníženy na nejnižší přiměřeně dosažitelnou míru a bez ohledu na jakákoli absolutní kritéria. U ojedinělých, ale velmi závažných rizik může být nutné přijmout opatření, která nejsou z přísně ekonomického hlediska odůvodnitelná.

Je nutné rovněž brát v úvahu existující opatření, která mohou mimo jiné přesahovat současné potřeby. Při úvahách nad odstraněním nadbytečných nebo zbytečných opatření je nutné zvážit, že se opatření mohou navzájem ovlivňovat. Kromě toho může být v některých případech levnější nadbytečná nebo zbytečná opatření ponechat, než je odstranit.

Při stanovování způsobů ošetření rizik by se mělo přihlížet:

- K tomu, jak riziko vnímají dotyčné strany,
- k nejvhodnějším způsobům, jak s těmito stranami komunikovat.

Výstupem tohoto kroku je plán ošetření rizik a zbytková rizika vyžadující rozhodnutí vedoucích pracovníků organizace o jejich akceptaci. (2)



Obr. 4: Přiměřená míra rizika – vztah mezi náklady na opatření a potenciálními škodami. Zdroj: (10)

2.6.8.1 Modifikace rizik

Vyberou se vhodná a odůvodněná opatření ke splnění požadavků identifikovaných v rámci posouzení a ošetření rizik. Tento výběr by měl brát v úvahu kritéria akceptace rizik a právní, regulační i smluvní požadavky. Opatření může zajistit jeden nebo více z následujících typů ochrany: Nápravu, vyloučení, prevenci, minimalizaci dopadu, odstrašování, odhalení, obnovení, monitorování a povědomí. Během výběru opatření je nutné zvážit náklady na získání, zavedení, správu, provoz, monitorování a údržbu opatření ve vztahu k hodnotě chráněných aktiv. (2)

Nad vše výše uvedené ještě existuje mnoho omezení, jež mohou ovlivnit výběr opatření.

- Časová omezení
- Finanční omezení
- Technická omezení
- Provozní omezení
- Kulturní, etická a ekologická omezení
- Právní omezení
- Snadnost použití
- Osobní omezení

2.6.8.2 Podstoupení rizik

„Jestliže úroveň rizika splňuje kritéria akceptace rizik, není zapotřebí přijímat další opatření a riziko lze podstoupit.“ (2)

2.6.8.3 Vyhnutí se riziku

Jsou-li identifikovaná rizika příliš vysoká, nebo převyšují-li náklady na uplatnění jiných způsobů ošetření rizik přínosy, organizace může přijmout rozhodnutí o celkovém vyhnutí se riziku tím, že od činnosti, jež dává riziku možnost vzniknout, upustí, nebo změní podmínky, za nichž tuto činnost provozuje. (2)

2.6.8.4 Sdílení rizik

Sdílení rizik zahrnuje rozhodnutí sdílet určitá rizika s externími stranami. Sdílení rizika může vytvářet nová rizika nebo měnit ty existující, již identifikovaná. Sdílení rizika lze provést například pojištěním. Obvykle není možné sdílet odpovědnost za dopad. (2)

2.6.9 Akceptace rizik

Plány ošetření rizik by měly popisovat, jak se mají hodnocená rizika ošetřit, aby vyhovovala kritériím akceptace rizik. Kritéria akceptace rizik mohou být komplexnější, než jen aby určovala, zda zbytkové riziko spadá či nespadá nad nebo pod určitou prahovou úroveň. V některých případech nemusí úroveň zbytkového rizika vyhovovat kritériím akceptace rizik, protože kritéria neberou v úvahu převažující okolnosti. Je-li to nutné, ti, kdo rozhodují, by měli explicitně uvést komentář k těmto rizikům s odůvodněním pro svoje rozhodnutí o tom, proč na běžná akceptační kritéria rizik nedbali.

Výstupem je seznam akceptovaných rizik s odůvodněním pro ta, která nesplňují běžná kritéria akceptace rizik organizace. (2)

2.6.10 Komunikace a konzultace rizik

Komunikace rizik je činnost vedoucí k získání dohody o tom, jak řídit rizika výměnou nebo sdílením informací o rizicích mezi těmi, kdo rozhodují, a ostatními zainteresovanými stranami. Tyto informace zahrnují mimo jiné existenci, charakter, formu, pravděpodobnost závažnost, ošetření a přijatelnost rizik. Výstupem tohoto bodu je trvalé chápání procesu řízení rizik bezpečnosti informací organizace a výsledků procesu. (2)

2.6.11 Monitorování a přezkoumávání rizik

Měla by být monitorována a přezkoumávána rizika a jejich faktory, aby bylo možné v raném stádiu identifikovat jakékoli změny v kontextu organizace a udržovat přehled komplexního obrazu rizik.

Organizace by měla zajisti neustále monitorování:

- Nových aktiv, která byla zařazena do rozsahu řízení rizik
- Nutných změn hodnot aktiv
- Nových hrozeb, které by mohly působit zvenčí i uvnitř organizace a které ještě nebyly hodnoceny
- Možnosti, že by nové nebo zvýšené zranitelnosti mohly umožnit hrozbám tyto nové nebo změněné zranitelnosti využít
- Identifikovaných zranitelností k určení těch, jež začínají být vystaveny nový nebo znovu se opakujícím hrozbám
- Zvýšeného dopadu následků hodnotových hrozeb, zranitelností a rizik, které dohromady způsobují nepřijatelnou úroveň rizik
- Incidentů bezpečnosti informací

Dále by měl být neustále monitorován, přezkoumáván a zdokonalován i proces řízení rizik podle toho, jak je to nutné a vhodné. Tato činnost přezkoumávání by měla řešit (nejen):

- Právní a ekologický kontext
- Kontext obchodní soutěže
- Přístup k posouzení rizik
- Hodnotu a kategorie aktiv
- Kritéria dopadu, vyhodnocení rizik a akceptace rizik
- Celkové náklady na vlastnictví
- Nutné zdroje.

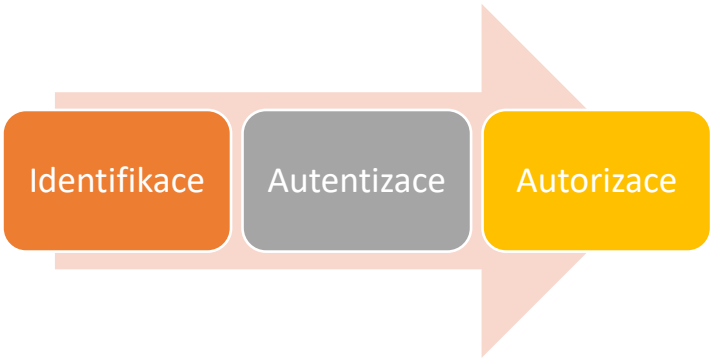
Organizace by měla zajistit, aby byly stále k dispozici zdroje pro posouzení a ošetření rizik, aby bylo možno přezkoumávat rizika, řešit nové nebo změněné hrozby nebo zranitelnosti a informovat o tom vedení organizace.

Monitorování řízení rizik může vyústit v pozměnění nebo doplnění používaného přístupu, metodiky nebo nástrojů v závislosti na identifikovaných změnách, opakování posouzení rizik, cíli procesu řízení rizik a předmětu procesu řízení rizik.

Díky tomu je zajištěna neustálá platnost procesu řízení rizik ve vztahu k obchodním cílům organizace nebo aktualizace procesu. (2)

2.7 Řízení přístupu

Řízení přístupu se z hlediska fungování opírá o tři základní prvky, identifikaci, autentizaci a autorizaci. Identifikace je proces umožňující rozpoznání entity na základě nějaké informace unikátní pro danou skupinu entit. Unikátní informací může být například uživatelské jméno, biometrický údaj, kód (ID) čipové karty. Autentizací se rozumí ověření proklamované identity identifikované entity (subjektu). Autentizace znamená *ověřování pravosti*, zajišťuje ochranu před falšování identity (subjekt se vydává za jiný subjekt, jímž ve skutečnosti není). Autorizace znamená oprávněnost, autorizujeme-li tedy uživatele, znamená to, že ho k něčemu oprávníme. O autorizaci hovoříme, chce-určitá entita přistupovat k daným zdrojům. Aby mohla k těmto zdrojům přistoupit, musí k tomu být oprávněna – autorizována. Předpokladem autorizace je úspěšná autentizace.



Obr. 5: Řízení přístupu. Zdroj: Vlastní

V praxi, pokud uživatel přistupuje k nějakému objektu, nejprve se identifikuje – sdělí svoje ID, následně se autentizuje – například pomocí hesla nebo PIN kódu. Poslední fází je autorizace, kdy se na základě již ověřené identity zjišťuje, zda má tento konkrétní uživatel oprávnění k provedení požadované akce, jak je ukázáno na Obr. 5. Některé systémy, například biometrické, mohou fázi identifikace a autentizace spojit do jednoho kroku. (24).

3 Analýza současného stavu

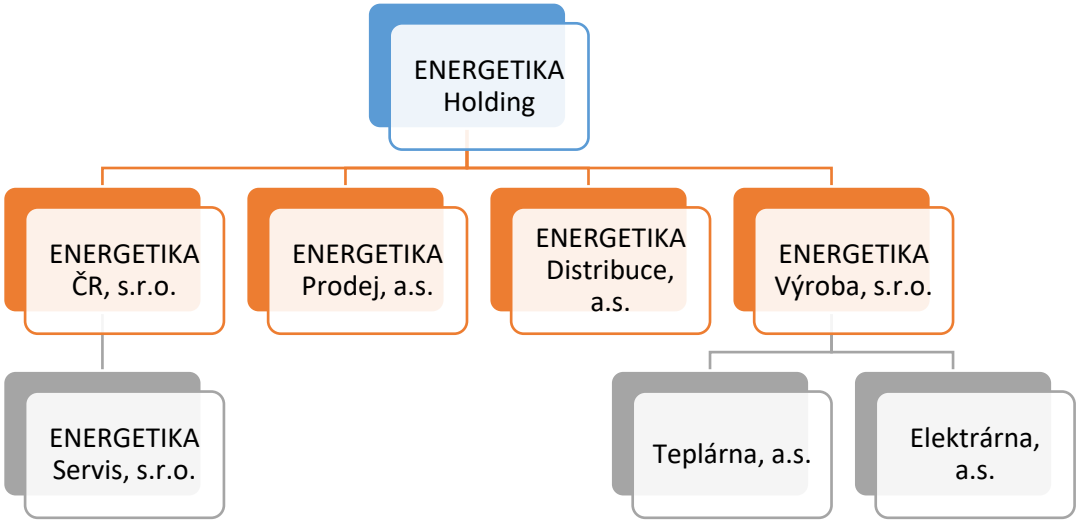
V analytické části bude nejprve představena vybraná společnost, pro niž je tato diplomová páce zpracovávána, následně bude provedena analýza současného stavu ochrany prvků kritické infrastruktury a řízení přístupu k nim, stejně jako ochrana dalších objektů společnosti a řízení přístupu k nim.

3.1 Popis společnosti

Vybraná energetická společnost, pro niž je tato diplomová práce zpracovávána, si z důvodu ochrany citlivých informací a údajů nepřeje být v práci explicitně jmenována. V práci bude proto vybraná společnost, resp. skupina společností označena zástupným jménem ENERGETIKA.

3.1.1 Struktura holdingu

Celý holding ENERGETIKA Holding je součástí nadnárodní korporace zabývající se energetikou na území celé Evropy. Skupina společností má z důvodů daných Evropskou směrnicí o společných pravidlech pro vnitřní trh s elektřinou (25) a Energetickým zákonem (3) následující holdingovou strukturu (zjednodušeno, pozměněné názvy):



Obr. 6: Holdingová struktura společnosti ENERGETIKA. Zdroj: Vlastní zpracování

Jednotlivé společnosti v rámci skupiny mají následující předměty podnikání:

- ENERGETIKA ČR, s.r.o.: Zastřešující organizace, ostatním společnostem skupiny poskytuje některé služby, majetek a prostory. Dle výroční zprávy zaměstnávala tato společnost v roce 2015 zhruba 1200 zaměstnanců (26).

- ENERGETIKA Prodej, a.s.: Prodej elektřiny a zemního plynu pro domácnosti, podniky i obce, revize a servis. Dle výroční zprávy zaměstnávala tato společnost v roce 2015 zhruba 250 zaměstnanců (27).
- ENERGETIKA Distribuce, a.s.: Provozovatel a vlastník elektrické distribuční soustavy a plynové distribuční soustavy. Držitel licence na distribuci elektřiny a plynu dne Energetického zákona (3). Dle výroční zprávy zaměstnávala tato společnost v roce 2015 kolem 50 zaměstnanců (28).
- ENERGETIKA Servis, s.r.o.: Opravy a údržba distribučních sítí, obsluha měřidel, výstavba veřejného osvětlení a další neregulované činnosti. Dle výroční zprávy zaměstnávala tato společnost v roce 2015 téměř 1000 zaměstnanců (29).
- ENERGETIKA Výroba, s.r.o.: Zastřešující organizace vlastnící jednotlivé výrobní jednotky (solární elektrárny, teplárny). V rámci transformace koncernu byli všichni její zaměstnanci převedeni do jiných společností v rámci skupiny (30), nebudeme se jí tedy dále zabývat.

Od roku 2018 bude skupina transformována do následující podoby:

- ENERGETIKA ČR, s.r.o. ze sebe oddělí svoji část do distribuční společnosti (projektanti, technici a další). Zbytek společnosti si zachová původní poslání, očekává se, že v ní zůstane asi 800 zaměstnanců.
- ENERGETIKA Distribuce, a.s. pojme navíc všechny zaměstnance společnosti ENERGETIKA Servis, s.r.o. a zhruba polovinu zaměstnanců ENERGETIKA ČR, s.r.o. včetně jejich zaměření a pracovní náplně. Vznikne tak společnost zaměstnávající zhruba 1900 lidí, jejímž předmětem podnikání bude vlastnictví a správa distribuční sítě, její výstavba a údržba, včetně projektování nových tras či připojování jednotlivých nových zákazníků.
- ENERGETIKA Prodej, a.s. zůstane zachována ve stávající podobě, očekává se nárůst počtu zaměstnanců na zhruba 300.

3.1.2 Působení společnosti v České republice

Holding ENERGETIKA na českém trhu působí od 90. let 20. století, kdy postupně nákupem akcií a akvizicemi získala majoritu ve společnostech, které zajišťovaly distribuci a prodej elektrické energie a zemního plynu v jednotlivých územních (nikoli samosprávných) krajích České republiky. Tyto regionální společnosti byly postupně

integrovány do holdingové struktury a následně, aby bylo vyhověno legislativním požadavkům při vstupu do Evropské unie (25), transformovány do současné podoby.

Společnost ENERGETIKA v současné době dodává na otevřeném trhu elektrickou energii více než 1 milionu zákazníků a zemní plyn více než 200 000 zákazníků. Elektrická distribuční síť vlastněná společností ENERGETIKA Distribuce, a.s. pokrývá území obývané cca 2 800 000 obyvateli, plynová distribuční síť pokrývá cca 800 000 obyvatel (31). Součástí holdingu ENERGETIKA je i několik elektráren a tepláren.

3.2 Objekty využívané společností

Skupina ENERGETIKA Holding provozuje a spravuje značné množství budov. Téměř v každé obci s rozšířenou působností na svém distribučním území má alespoň služebnu, kde se nachází technický personál. Zpravidla v bývalých okresních městech se pak nacházejí administrativní budovy, kde pracují regionální technici starající se o rozvoj sítě v daném okrese a prodejci. Nad tím vším, v sídlech původních regionálních společností sídlí týmy s celofiremní působností (IT, HR, call centrum, facility management a další).

Samostatnou kapitolou jsou pak objekty přímo související s distribucí elektrické energie, tedy rozvodny. Ty se nachází v blízkosti větších sídel, případně v blízkosti velkých odběratelů energie, přímo sousedí s elektrárnami nebo s rozvodnami přenosové soustavy provozovanými společností ČEPS, a.s. Dále bychom ve výčtu mohli pokračovat trafostanicemi ještě trafostanicemi, které zásobují menší celky, je jich tedy značné množství. Úroveň samotného vedení či kabelových tras bude zmíněna pouze okrajově.

Tato podkapitola si nebere za cíl být kompletním výčtem všech nemovitostí skupiny ENERGETIKA v České republice, chce být pouze přehledem nejčastějších typů těchto budov.

3.2.1 Administrativní centra

Velká administrativní centra společnosti se nachází v krajských městech bývalých územních (nikoli současných samosprávných) krajů. Prakticky se jedná o původní budovy ředitelství bývalých regionálních energetických společností.

V těchto budovách se pohybují pracovníci snad všech společností skupiny, někteří na denní bázi, jiní při pravidelných školeních nebo jiných událostech. Do těchto budov má rovněž zájem vstupovat značné množství lidí, kteří nejsou zaměstnanci skupiny. Může se

jednat o agenturní pracovníky (call centrum), externí dodavatele (tisk, část IT, úklid), zákazníky či jiné osoby, které mají oprávněný důvod se po budovách pohybovat. Administrativní centra jsou vybavené recepcí, kde je přítomen pracovník ostrahy (zaměstnanec externí firmy) proškolený tak, aby mohl návštěvníky (zákazníky) správně nasměrovat a některé i sám odbavit (například doporučením konkrétního formuláře a pomoci s jeho vyplněním).

Jedná se o budovy lokalizované v městské zástavbě. Často k budovám náleží neveřejná parkoviště vyhrazená pro služební či soukromé vozy některých zaměstnanců.

V některých z administrativních centrech je zaveden systém využívající čipové karty. Ty jsou používány k identifikaci zaměstnanců a ovládání zastřežení budovy. Návštěvníkům jsou vydávány čipové karty pro hosty, které umožňují přístup do některých částí objektu, bohužel nikoli selektivně, ale rovnou do všech, kam vůbec mohou mít návštěvníci přístup.

V administrativních centrech je zaveden poplachový zabezpečovací a tísňový systém. Pro jeho aktivaci a deaktivaci používají zaměstnanci svoje čipové karty v kombinaci s PIN kódem zadávaným pomocí klávesnice terminálu PZTS. V některých budovách jsou čipové karty používány pro přístup do některých částí těchto budov. Toto opatření bohužel není instalováno plošně. V administrativních centrech je zaveden kamerový systém se záznamem, který monitoruje vstup a vjezd do budovy a dále některé další prostory (kanceláře nikoli).

3.2.2 Administrativní budovy v dalších městech

Ve větších městech (zpravidla bývalých okresních) má společnost ENERGETIKA vlastní budovu, kde jsou soustředěni mimo jiné projektanti a jiní technici starající se o údržbu a rozvoj distribuční sítě v dané oblasti (okrese). Dále zde mají své kanceláře pracovníci zodpovědní za styk s velkými odběrateli v konkrétním regionu (okrese), správci majetku a další. Historicky se v těchto objektech nacházely i obchodní kanceláře společnosti ENERGETIKA. Jejich činnost v současné době supluje proškolená ostraha na recepcích těchto objektů a bezplatné telefonní spojení na zákaznickou linku společnosti.

I tyto administrativní budovy se nacházejí v běžné městské zástavbě, mohou mít vyhrazená parkoviště. Často mohou být součástí těchto objektů i služebny techniků

(montérů). I tyto objekty jsou vybaveny recepcí, kde je v pracovních dnech přítomen proškolený pracovník ostrahy (externí firma).

Administrativní budovy mají zavedeny podobná opatření jako administrativní centra. Je zde opět zaveden poplachový zabezpečovací a tísňový systém, který mohou zaměstnanci ovládat pomocí svých čipových karet a PIN kódu. Stejně jako v administrativních centrech je zde zaveden kamerový systém dohlížející na vstup a vjezd do objektu, případně některé chodby, prostor recepce a dvůr. Nebývá zde zaveden přístup pouze do určité části budovy za použití čipové karty.

3.2.3 Služebny

Služebny společnosti ENERGETIKA poskytují zázemí pro techniky (montéry), kteří se starají o údržbu a opravy distribuční sítě. Služebny musí poskytovat prostor pro služební vozidla techniků (osobní vozy, dodávky, vysokozdvižné plošiny, měřící vozy aj.). Dále jsou vybaveny skladem nejčastěji používaného materiálu. Na služebně samozřejmě nesmí chybět zázemí pro techniky, tedy kanceláře, kuchyňka a sociální zařízení.

Služebny se zpravidla nacházejí v okrajových částech měst, nikoli v jejich centrech. Mohou ale být zároveň součástí výše zmíněných administrativních budov, případně níže zmíněných rozvoden. Samostatně se nejedná o prvek kritické infrastruktury (6).

Na služebny mají primárně přístup technici (montéři), dále pak pracovníci správy budov (facility management) a dodavatelé (materiálu, služeb). Pro žádné další osoby (zákazníky, návštěvy) nemá přístup do těchto objektů žádný smysl.

Je-li služebna součástí objektu jiné kategorie, sdílí s tímto objektem přístupový systém. Jedná se o služebny spojené s administrativními budovami ve městech, nebo naopak na rozvodnách.

Samostatně stojící služebny mají zpravidla instalován poplachový zabezpečovací a tísňový systém v budově se zázemím pro techniky, v garážích i ve skladech materiálu. K přístupu do objektů technici nepoužívají žádné čipové karty, ale běžné (skupinové) klíče. V případě, že do objektu služebny zavítá návštěva nebo jiná oprávněná osoba (dodavatel, nadřízený), zpřístupnění objektu je jí umožněno tak, že se s danou osobou po objektu pohybuje doprovod disponující oprávněními a prostředky k přístupu do

zabezpečených prostor. V samostatných služebnách zpravidla není zaveden kamerový systém.

3.2.4 Rozvodny

Společnost ENERGETIKA spravuje vlastní rozvodny distribuční soustavy (stanice typu 110/22 kV), které jsou dle Nařízení vlády č. 315/2014 Sb. zařazeny mezi prvky Kritické infrastruktury České republiky.

Tyto stanice se zpravidla nacházejí na okrajích větších sídel či v blízkosti velkoodběratelů, v těsné blízkosti elektráren nebo rozvoden Přenosové soustavy (stanice 400/110 kV nebo 220/110 kV)

Do objektů rozvoden mají přístup pouze pověřené a k tomu oprávněné osoby, tzv. rozvodní. Pokud je součástí rozvodny i Služebna, je rozvodna od zbylé části areálu fyzicky oddělena (plotem, zdí).

V současnosti je přístup do rozvoden řešen kombinací čipových karet a poplachového zabezpečovacího a tísňového systému a bezpečnostních zámků a klíčů. Čipové karty zde slouží k identifikaci pracovníka při aktivaci a deaktivaci PZTS, dále pro otevírání vjezdové brány do objektu. Na rozvodnách je instalován kamerový systém se záznamem. Společnost ENERGETIKA Distribuce, a.s. rozlišuje následující 4 typy rozvoden:

- R1 – Bez stálé obsluhy, manipulace dle požadavku dispečera, dálkové ovládání
- R2 – Kontrola 1× za 12 hodin, manipulace dle požadavku dispečera, dálkové ovládání
- R3 – Obsluha přítomna denně v čase 7 až 19 hodin, mimo tuto dobu bez obsluhy a kontrol, manipulace na požadavek dispečera, dálkové ovládání
- R4 – Trvalá obsluha 24 hodin denně

Fyzická ostraha je přítomna povinně je na rozvodnách kategorie R4.

3.2.5 Trafostanice

Trafostanice je zařízení, které za pomoci transformátoru přeměňuje vysoké napětí (22 kV) na nízké napětí (400 V, 230 V). Každá trafostanice je na jedné straně spojena s rozvodnou pomocí VN vedení, z ní pak vede NN vedení ke koncovým zákazníkům (zpravidla domácnostem). Větší odběratelé mohou disponovat vlastními trafostanicemi.

Trafostanice mohou mít podobu samostatného uzavřeného objektu, být integrovanou součástí jiného (i cizího) objektu, nebo mohou být postavené venku na sloupech. Do uzavřené trafostanice má přístup pouze technik (pomocí speciálního klíče), který do ní vstupuje pouze za účelem revize, údržby nebo opravy. Venkovní trafostanice jsou umístěny na sloupech v takové výšce, aby byly bez dalšího vybavení pro člověka těžko dosažitelné, zde se jedná o ochranu polohou.

3.2.6 Venkovní a kabelové vedení

Společnost ENERGETIKA spravuje celou distribuční soustavu na daném území, elektrický proud přes její vedení protéká od rozvodny přenosové soustavy (spravované společností ČEPS, a.s.) přes vlastní rozvodny distribuční společnosti a trafostanice až k elektroměru u zákazníka. Tento přenos je realizován pomocí venkovního vedení (VVN, VN, NN) a kabelového vedení (VN, NN).

Z hlediska rozmístění tras elektrického vedení lze konstatovat, že ho lze nalézt téměř všude, jak ve volné krajině, tak v sídlech. Tam, kde je zástavba hustší je vedení zpravidla realizováno podzemními kabely (mimo jiné i z estetických důvodů), přenos na delší vzdálenosti případně v řídce osídlených oblastech je realizován venkovním vedením.

Venkovní i kabelové vedení je navrženo tak, aby běžnému člověku při běžném chování nehrozil úraz elektrickým proudem a ani ho nemohl nijak poškodit, jedná se o ochranu polohou. Technici musí při údržbě a opravách elektrického vedení užít speciální prostředky (jak pro přístup, tak pro svoji ochranu). Přístup k těmto objektům nebude dále v této práci řešen.

3.2.7 Elektrárny

Skupina ENERGETIKA provozuje v současné době několik vodních a solárních elektráren, dále pak také několik desítek kogeneračních jednotek pro výrobu elektřiny a tepla. Do elektráren má přístup pouze jejich obsluha a případně další oprávnění pracovníci. Běžný zákazník nebo občan do elektrárny nemá přístup. Výjimkou jsou informační centra elektráren a případné školní a jiné exkurze do výrobních částí elektráren.

Fyzické zabezpečení elektráren je zajištěno běžnými prostředky, tedy plotem (případně zdí), bránou, dveřmi se zámky. V případě potřeby není nutná přítomnost obsluhy v některých elektrárnách, lze je totiž ovládat dálkově.

Žádnou z elektráren skupiny nelze dle Nařízení vlády č. 315/2014 Sb. označit za prvek Kritické infrastruktury, neboť nesplňují požadavek na minimální instalovaný výkon. Samotná vodní díla, na kterých jsou elektrárny postaveny, však již prvky KI být mohou, nejsou však majetkem skupiny ENERGETIKA. Na druhou stranu, některé vodní elektrárny skupiny ENERGETIKA jsou součástí krizových scénářů pro případ rozpadu přenosové a distribuční sítě (blackout) jako záložní zdroje schopné pokrývat vlastní spotřebu jaderných elektráren v České republice. Z tohoto hlediska je lze jako prvek KI označit i společně s některými rozvodnami, jejichž pomocí bude sestavena přímá trasa mezí vodní a jadernou elektrárnou.

Řízení přístupu do elektrárny je prakticky shodné s rozvodnou – kombinace poplachového zabezpečovacího a tísňového systému, čipové karty a klíčů. V elektrárnách je instalován kamerový systém se záznamem.

3.2.8 Rekreační objekty

Pro úplnost uvedeme, že skupina ENERGETIKA disponuje i několika vlastními rekreačními objekty, jejichž kapacity jsou nabízeny k rekreaci primárně zaměstnancům a jejich příbuzným, případně, je-li kapacita nevyužitá, i dalším osobám. Jedná se většinou o větší chaty (v horách, u vodních ploch), případně části školících středisek (historické objekty v atraktivních lokalitách).

Správcem objektu je zpravidla místní občan, který je pro tuto činnost najat jako externí pracovník. Přístup do rekreačních objektů řídí správce objektu, který vydává rekreantům klíče od objektu/pokojů. Rekreační objekty jsou vybaveny poplachovým zabezpečovacím a tísňovým systémem napojeným na pult centrální ochrany, který je schopen v případě narušení vyslat k objektu zásahovou jednotku. Přístup k těmto objektům nebude dále v této práci řešen.

3.3 Stávající systém fyzické ochrany

Společnost ENERGETIKA již ve svých objektech samozřejmě nějaký systém fyzické ochrany používá. Tento fakt může realizaci nového přístupového systému na jednu stranu

zjednodušit – využije se stávající systém a vhodně se doplní, na druhou stranu může stejně tak návrh nového systému zkomplikovat – zastaralé nebo různé systémy v jednotlivých objektech.

3.3.1 PZTS

Pravdou je, že v dřívější době, ještě před transformací jednotlivých regionálních energetických společností do holdingu ENERGETIKA byly zabezpečovací systémy realizovány v různých městech různými dodavateli. Po začlenění do holdingu byly systémy PZTS a zaměstnanci fyzické ostrahy převedeni pod jednu dodavatelskou společnost. Na její pulty centrální ochrany jsou napojeny všechny PTZS v jednotlivých objektech a zároveň jsou všichni strážní jejími zaměstnanci (před začleněním do holdingu ENERGETIKA byli zaměstnáni přímo v regionálních energetických společnostech, tedy nebylo využíváno outsourcingu této služby). PTZS je zaveden ve všech administrativních budovách, v rozvodnách a elektrárnách, ve většině služeben a v některých významnějších trafostanicích.

3.3.2 Fyzická ostraha

Fyzická ostraha nebo vrátenská služba je přítomna v administrativních objektech po dobu jejich otevíracích hodin (zpravidla 6:00 až 18:00), dále je přítomna v některých rozvodnách (tam, kde je přítomna i fyzická obsluha v režimu 24/7).

3.3.3 CCTV

Kamerový systém CCTV je provozován ve všech administrativních budovách, na některých služebnách a na některých rozvodnách (kategorie R4 povinně, ostatní volitelně). Záznamové zařízení CCTV pro ukládání záznamů bývá situováno přímo v daném objektu. Na některých místech jsou namísto kamer CCTV použity atrapy kamer.

3.3.4 Systém kontroly vstupu

Systém kontroly vstupu je implementován v některých velkých administrativních centrech, kde se zaměstnanecké karty používají pro vstup do některých částí těchto objektů. Bohužel je současný stav takový, že vlivem občasného stěhování některých oddělení v rámci budovy se rozšiřují zóny, kam se s každou jednotlivou kartou dá dostat, ale nemažou se ty již nepotřebné. Je tedy velmi pravděpodobné, že někteří zaměstnanci mají přístup téměř všude (v rámci objektu nebo i několika objektů), i když by tam přístup

mít neměli. Dále je systém kontroly vstupu implementován jako součást PTZS v budovách rozvoden. Rovněž využívá zaměstnanecké karty, tentokrát pro deaktivaci a aktivaci detekčních zón. Pokusy o neoprávněný přístup jsou detekovány, přenášeny na dohledové pracoviště a zaznamenávány. V rozvodnách lze systém použít i bez zaměstnanecké karty pomocí zadání zvláštního PIN kódu na klávesnici. Systém je v rozvodnách provozován současně s bezpečnostními dveřními zámky (minimálně bezpečnostní třída 3 dle ČSN EN 1627).

Všechny brány, branky, vstupní dveře do skladů a dalších objektů rozvodny, které jsou zabezpečeny i pomocí PZTS, by měly být vybaveny elektrickým zámkovým systémem. Zámky jsou prioritně ovládány systémem kontroly vstupů s definovaným oprávněním pro vstup osob a vjezd vozidel. Pro případ jakékoli poruchy, závady nebo nefunkčnosti elektrického ovládání zámků a ostatních elektromechanických pohonů a prvků pro vstupy do objektů musí být vždy zachována možnost ovládání zámků pomocí mechanických klíčů. Zda tomu tak je opravdu ve všech rozvodnách by mělo být předmětem detailnější analýzy, která ale není předmětem této práce.

Odemknutí a otevření klíčem (nouzové použití klíče) je signalizováno formou poplachové zprávy a přenášeno na dohledové pracoviště. Všechny zámkové systémy musí minimálně splňovat požadavky bezpečnostní třídy č. 3 dle ČSN EN 1627.

V administrativních budovách zpravidla existuje systém skupinových klíčů a systém generálního klíče. Skupinové klíče mohou používat například správci budov (facility management), úklidová služba a další. Generální klíč je k dispozici u ostrahy.

Trafostanice jsou opatřeny zpravidla visacím zámkem případně cylindrickou vložkou. K přístupu do nich se používají speciální klíče, které jsou pro všechny trafostanice společné (v určité oblasti). Služebny jsou vybaveny běžnými zámky, jsou zavedeny skupinové klíče.

3.4 Analýza SLEPT

Analýza SLEPT je prostředkem pro analýzu obecného okolí společnosti.

3.4.1 Sociální faktory

Zavedení nového přístupového systému či jeho změna ve všech objektech skupiny ENERGETIKA se přímo nebo dotkne prakticky všech obyvatel regionů, ve kterých se

objekty (budovy a zařízení) společnosti nacházejí. Při jeho návrhu je nutné tento fakt zohlednit.

Nejvíce zasaženou skupinou budou samotní zaměstnanci holdingu ENERGETIKA, respektive jeho jednotlivých dceřiných společností. Jedná se zhruba o 2500 osob ve věku 18 až 65 let obou pohlaví. Tito lidé budou každodenními uživateli systému, měl by tedy být navržen tak, aby jeho používání nebylo pro zaměstnance příliš obtěžující.

Druhou dotčenou skupinou jsou zákazníci, dodavatelé a další návštěvy. Jedná se například o zákazníky, kteří přijdou s techniky společnosti vyřizovat zřízení odběrného místa nebo podobné záležitosti, případně dodavatelské firmy řešící například drobné opravy uvnitř objektu.

Třetí, nejméně dotčenou skupinou jsou všichni obyvatelé regionů, kde holding ENERGETIKA působí. Tito obyvatelé se mohou běžně pohybovat v okolí objektů společnosti. Zabezpečení především distribučních a výrobních objektů proto musí tento fakt reflektovat a zamezit neoprávněnému, úmyslnému či neúmyslnému vniknutí nepovolaných osob do objektů, ideálně již ve fázi plánování takových činů.

3.4.2 Legislativní faktory

Na holding ENERGETIKA, jakožto subjekt KI dle *Nařízení vlády č. 432/2010 Sb.* se vztahuje nespočet různých regulací, norem a zákonů. Mimo jiné jde o *Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů* (dále jen Krizový zákon). Ten mimo jiné ukládá subjektu kritické infrastruktury odpovědnost za ochranu prvku kritické infrastruktury. (19) (7)

Konkrétní požadavky na zabezpečení prvku KI specifikuje norma ČSN P 73 4450-1. (4)

Jako dodavatel a distributor energií pak také společnost podléhá regulaci ze strany Energetického Regulačního Úřadu. (3)

Nově pak také holding ENERGETIKA spadá do sféry vlivu *Zákona o kybernetické bezpečnosti (181/2014 Sb.)*, jelikož její informační systémy lze zařadit mezi systémy Kritické Informační Infrastruktury (KII). (5)

Na provozování přístupového systému a sběru dat z něj má zcela jistě vliv i *Zákon č. 101/2000 Sb. o ochraně osobních údajů.* Je však vhodné vzít v úvahu i *Nařízení*

Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů – Obecné nařízení o ochraně osobních údajů (GDPR – General Data Protection Regulation), které vstoupí v platnost v květnu 2018 a bude závazné pro všechny členské země EU, tedy i pro holding ENERGETIKA. (22) (23)

3.4.3 Ekonomické faktory

Vnější ekonomické faktory působící na projekt realizace změny přístupového systému do objektů holdingu ENERGETIKA lze jen těžko hledat. Vliv může mít míra zdanění pracovní síly, která tuto změnu může realizovat. Naopak zcela nulový vliv bude mít výše DPH, neboť všechny nově pořizované prvky budou nakupovány za ceny bez DPH. Nejzásadnějším ekonomickým faktorem pak je ten vnitřní – financování nového přístupového systému ze strany Společnosti.

3.4.4 Politické faktory

Politické faktory úzce souvisí s ekonomickými a legislativními. Jsou to totiž právě politici, kdo ovlivňuje, jaká bude výše zdanění pracovní síly, daně a další. Rovněž politická reprezentace rozhoduje o přijímání závazných norem.

Normy, jimž by měl nový přístupový systém odpovídat (GDPR, kybernetický zákon) jsou relativně nové a neočekává se jejich brzká změna. Krizový zákon a jeho prováděcí vyhláška jsou sice staršího data vydání, ale jsou natolik obecné, že by jejich případná drobná změna neměla ovlivnit návrh systému, a velká změna by neměla nastat.

3.4.5 Technologické faktory

Technologie v oblasti zabezpečovacích systémů a fyzické bezpečnosti objektů prochází postupnou evolucí, nikoli však revolucí. V poslední době se objevují nové metody identifikace uživatele – k otisku prstu či dlaně se přidává sken oční duhovky krevního řečiště. Samozřejmě nadále existují čipové karty či jiné přístupové tokeny, používají se elektromechanické klíče. Experimentuje se s čipy voperovanými do lidského těla, kde však technologie naráží na značný odpor potenciálních uživatelů z důvodu strachu o soukromí.

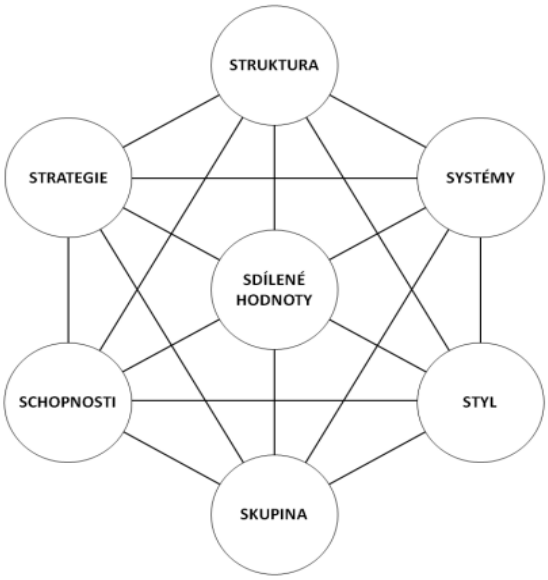
Dohledové kamerové systémy mají nové možnosti – vyšší rozlišení, noční vidění, termovize. To však klade stále vyšší požadavky na ukládání a ochranu velkého množství

dat. Tato data je potřeba adekvátně uchovávat, klasifikovat a po určité době též adekvátně likvidovat. Zároveň je nutné zamezit přístupu neoprávněných osob k těmto datům.

Co se týče samotných fyzických bezpečnostních prvků, probíhá postupný vývoj bezpečnostních dveří, oken, zámků a dalších prvků, a to především z hlediska jejich odolnosti proti neoprávněnému vniknutí nebo například požární ochrany.

3.5 Analýza interních faktorů – model McKinsey 7S

Analýza 7S byla navržena v 70. letech 20. století konzultanty z americké společnosti McKinsey&Company, podle níž se tato analýza jmenuje. Do hodnocení jsou zahrnuty faktory zmíněné na Obr. 7 a blíže popsané v následujících podkapitolách. (32)



Obr. 7: Rámec 7S faktorů firmy McKinsey. Zdroj: (32)

3.5.1 Strategie

Cílem projektu je návrh přístupového systému do objektů prvků kritické infrastruktury a dalších objektů holdingu. Tento systém by měl splňovat nejen legislativní požadavky dle dříve zmíněných zákonů, ale být i přínosem pro jeho uživatele, ať už samotnou Společnost, nebo její zaměstnance a zákazníky.

Strategií společnosti jako takové je udržovat a rozvíjet distribuční a přenosovou soustavu na spravovaném území a být minimálně v těchto regionech jedničkou na trhu dodavatelů energií.

3.5.2 Struktura

Struktura společnosti je holdingová. Některé z dceřiných firem ve skupině jsou akciové společnosti, jiné společnosti s ručením omezeným. Jednotlivé dceřiné společnosti v rámci skupiny mají svůj vlastní předmět podnikání, například:

- Nákup a prodej elektrické energie a plynu
- Provozování elektrické a plynové distribuční soustavy
- Provoz a údržba distribučních sítí
- Zajišťování IT a HR pro zbytek skupiny

Dále, jednotlivé elektrárny a teplárny jsou samostatnými společnostmi v rámci skupiny.

Systém řízení jednotlivých společností v rámci skupiny je pro projekt návrhu přístupového systému irelevantní. Projekt návrhu systému řeší projektový tým ze společnosti ENERGETIKA ČR, s.r.o.

Některé společnosti v rámci skupiny mezi sebou sice sdílí některé objekty, ale přístupová práva budou přidělována přímo konkrétním zaměstnancům či skupinám zaměstnanců.

3.5.3 Systémy

Jedná se o jádro celého projektu. V současné době v některých objektech, spíše těch administrativních existuje jistá forma přístupového systému pomocí čipových karet. V objektech KI je přístupový systém zaveden částečně a značně nesystémově rozvíjen, často v kombinaci se systémem speciální systém zámků a klíčů a elektronických zabezpečovacích zařízení (alarm).

3.5.4 Systém řízení

Za řešení projektu je odpovědný projektový tým vedený projektovým manažerem. Ten se zodpovídá svému nadřízenému, jímž je ředitel dané divize.

Jednotlivé společnosti v rámci skupiny mají různé systémy řízení dle povahy svého zaměření. Servisní společnost má například liniovou strukturu, obchodní spíše maticovou. Pro realizaci našeho projektu je však toto členění irelevantní.

3.5.5 Spolupracovníci

Ve všech společnostech v rámci skupiny ENERGETIKA se pohybuje značné množství osob (cca 2500 zaměstnanců) různých profesí. Jedná se montéry, techniky, odborníky pro

práce ve výškách nebo pod napětím, dále projektanty, rozpočtáře, administrativní pracovníky, obchodní zástupce, operátory call centra, IT profesionály, manažery, ředitele, procesní inženýry a další profese běžné v korporátním prostředí.

Nábor nových zaměstnanců probíhá různými formami, opět podle zaměření. Na některé pozice společnost ENERGETIKA ČR, s.r.o. přijímá agenturní pracovníky, jiné si vytipovává už na specializovaných středních školách a zavazuje si je pomocí stipendií. Pro vysokoškolské studenty nabízí pracovní stáže a trainee programy.

Zaměstnanci pravidelně prochází školeními, a i přezkoušeními podle svého zaměření (například vyhláška č. 50/1978 u techniků), mají možnost jazykových kurzů a podobně. Většina zaměstnanců je členem odborového svazu.

3.5.6 Schopnosti

Společnost, tedy skupina společností je jedním z předních dodavatelů elektrické energie a zemního plynu v České republice. Mimo to spravuje značnou část přenosové soustavy České republiky. Nad rámec těchto služeb se společnost ENERGETIKA Prodej, a.s. snaží nabídnout svým zákazníkům další přidanou hodnotu pomocí slev nebo dotací na úsporné produkty šetřící energie nebo další bonusy s pomocí různých aliančních partnerů z oblasti maloobchodu, bankovnictví nebo pojišťovnictví.

3.5.7 Sdílené hodnoty

Společnost se velmi angažuje hlavně v ekologických projektech, je partnerem soutěže přezdívané „Ekologický Oskar“, podporuje a propaguje rozvoj elektromobility a vozů na stlačený zemní plyn (CNG). Podporuje a propaguje rovněž nové chytré technologie, s jejichž pomocí lze šetřit energie, životní prostředí i čas (například projekt Smart City).

Společnost má zavedený Etický kodex a zpracovanou společenskou zodpovědnost. Je partnerem mnoha kulturních nebo sportovních akcí.

Implementace našeho projektu přístupového systému do těchto hodnot zapadá minimálně v oblasti ochrany zdraví – zabránění přístupu nepovolaných osob tam, kde by si mohly ublížit.

3.6 Analýza rizik současného stavu

Z katalogu hrozeb uvedených v Příloze 8 této práce vybíráme podmnožinu hrozeb vztahujících se k fyzické bezpečnosti, konkrétně přístupovému systému a stavu, kdy by byl zaveden částečně nebo vůbec. Za jistých okolností by zde bylo možné vyjmenovat všechny hrozby uvedené v katalogu, protože jsou možné jejich kombinace. Zaměříme se tedy spíše na ty přímo související. U hrozeb jsou uvedeny příklady možných následků.

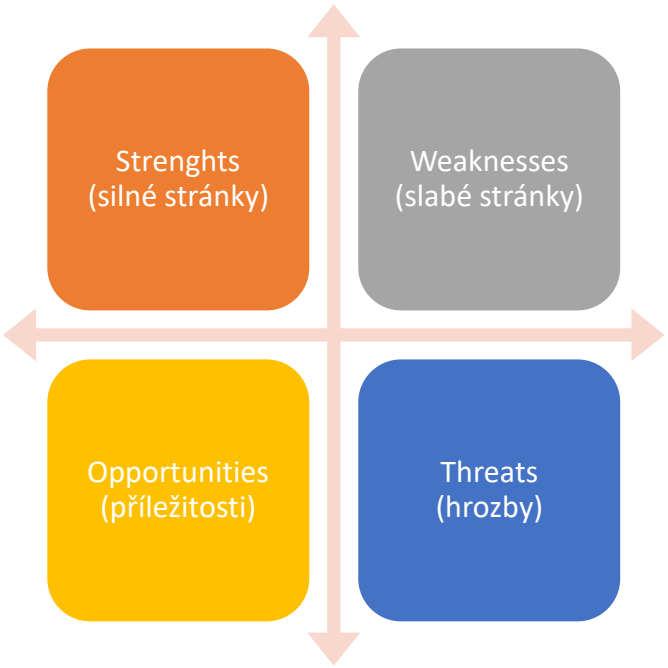
- Požár, povodeň, zemětřesení a další přírodní hrozby – hrozí poškození fyzické ochrany, uvíznutí osob uvnitř objektu
- Přerušení dodávky elektřiny, provozní porucha, selhání záložních zdrojů napájení – nefunkčnost PTZS, uvíznutí osob, nechráněná aktiva
- Selhání osvětlení v posuzovaném prostoru – zhoršená manipulace
- Technická selhání systémů FO – nefunkčnost PTZS, uvíznutí osob, nechráněná aktiva
- Organizační selhání (lidský faktor), chyby zaměstnanců – může vést k ohrožení života nebo možnosti úrazu, případně k ekonomickým ztrátám
- Ohrožení fyzické povahy (lidský faktor), tedy neoprávněné vniknutí do objektu a neoprávněná manipulace s aktivy – ekonomické ztráty, ohrožení života, nefunkční systémy, zničená či jinak znehodnocená aktiva, kompromitace smluv, osobních údajů a dalších informačních aktiv
- Terorismus (výhružky, únos, bomba, vydírání, držení rukojmí) – unesení zaměstnanci, zničená či jinak znehodnocená aktiva
- Logické hrozby (falšování identity, zneužití systémových prostředků) – neoprávněné užití zdrojů
- Krádež – ekonomická ztráta

Ze seznamu hrozeb a analýzy možných scénářů vyplývá, že lze provést určitá opatření, která by mohla snížit riziko těchto scénářů. Zabývat se jimi bude kapitola 4.

3.7 SWOT analýza projektu

Analýza SWOT shrnuje slabé a silné stránky, příležitosti a hrozby projektu *Návrh přístupového systému jako součást řešení fyzické bezpečnosti*. Analýza SWOT zkoumá čtyři oblasti: Silné stránky, Slabé stránky, Příležitosti a Hrozby, přičemž první dvě

označujeme jako interní, další dvě jako externí. Základní schéma analýzy SWOT je znázorněno na Obr. 8



Obr. 8: Základní schéma SWOT analýzy. Zdroj: Vlastní zpracování.

3.7.1 Silné stránky (vnitřní)

- Zázemí stabilní společnosti pro realizaci projektu
- Legislativou a normami dané požadavky
- V současnosti je již v některých objektech KI část systému implementována
- Realizaci provádí interní zaměstnanci společnosti (znalost vnitřních procesů)

3.7.2 Slabé stránky (vnitřní)

- Setrvačnost zaměstnanců a neochota přizpůsobit se změnám.
- V jednotlivých regionech, kde Společnost působí, se dosavadní zabezpečení a povědomí o něm značně liší
- Možný nedostatek zkušeností realizačního týmu s podobnými projekty
- Financování z vlastních zdrojů, investice nezvýší potenciální zisk společnosti

3.7.3 Příležitosti (vnější)

- Získání státní nebo jiné dotace na realizaci systému
- Možnost využití existujících prostředků (ploty, kamerové systémy a jiné)

- Nové technologie v oblasti identifikace osob

3.7.4 Hrozby (vnější)

- Změna legislativy
- Nekvalitně provedená práce subdodavatelem
- Neadekvátní návrh systému
- Nekompletní návrh systému

4 Vlastní návrh řešení

V této kapitole bude navrženo obecné řešení přístupového systému pro jednotlivé typy objektů, které bude následně předvedeno na Modelovém objektu zahrnujícím budovy různých typů určení (kategorií).

4.1 Identifikátory

V současné době se pro identifikaci zaměstnanců (a návštěvníků v některých objektech) používají čipové bezkontaktní karty. Nejsou to však jediné možnosti identifikace zaměstnanců pro řízení přístupu, dalšími mohou být:

- Čipy (kontaktní či bezkontaktní)
- Běžné klíče
- Skupinové klíče
- Mechatronické klíče
- Biometrické údaje (otisk prstu, duhovka, sítnice)
- Kombinace jména a hesla

Po sérii rozhovorů se zaměstnanci skupiny ENERGETIKA byly specifikovány následující požadavky, které budou dále podrobněji rozebrány.

1) Kompatibilita se stávajícím systémem při postupném zavádění
2) Na první pohled jasné rozlišení zaměstnance a návštěvníka
3) Možnost zpětně identifikovat zaměstnance podle identifikátoru
4) Možnost měnit přístupová práva zaměstnance při zachování stejného identifikátoru
5) Možnost dalšího využití, například pro systém sledování docházky, placení ve firemním stravovacím zařízení, odemykání sdílených vozidel a další.
6) Škálovatelnost systému (postupné zavádění)

4.1.1 Kompatibilita se stávajícím systémem

Z hlediska kompatibility se stávajícím systémem nejlépe vyhovuje pokračování v používání **bezkontaktních čipových karet** (tam, kde to má smysl) a **skupinových klíčů**. Bylo by možné pohodlně nahradit karty **bezkontaktními čipy** (přívěsky) využívajícími stejnou technologii. Kontaktní čipy již dnes téměř nedávají z uživatelského

hlediska smysl. Plošné zavedení mechatronických klíčů by vyžadovalo značnou investici, stejně jako zavádění čteček biometrických údajů (které by alespoň nevyžadovalo kompletní výměnu stávajících zámků). Podobné by to bylo s vybavováním všech míst, kde má být kontrolován vstup, klávesnicí pro zadání jména a hesla, nehledě na značný uživatelský diskomfort způsobený především zdlouhavostí zadávání.

4.1.2 Rozlišení zaměstnance a návštěvníka

V tomto bodě jde především o snadné a rychlé rozlišení, zda se jedná o zaměstnance skupiny ENERGETIKA či nějakou cizí osobu. Identifikátor tedy musí být dobře viditelný a viditelně nositelný. Proti čipům a klíčům jasně mluví jejich malé rozměry a možná případná neochota dodávat je ve více barvách. Biometrické údaje zde odpadají úplně, podle nich nelze laickým pohledem ihned poznat, zda se jedná o zaměstnance nebo někoho jiného (obzvlášť v hlavních budovách s větším počtem zaměstnanců a větším pohybem lidí), neznáme-li danou osobu. Jednoznačnou volnou z tohoto pohledu by měly být **bezkontaktní karty**. Je velmi jednoduché vytvořit například červené karty s nápisem „Návštěva, doprovod nutný“, zatímco zaměstnanci mají karty bílé s vlastní fotografií.

4.1.3 Možnost zpětně identifikovat zaměstnance podle identifikátoru

Biometrické údaje zde vynecháme jako irelevantní. Zde bych se opět klonil k použití **bezkontaktních čipových karet**. Lze na ně jednoduše vytisknout nebo nalepit štítek se jménem a fotografií zaměstnance a jeho pracovním zařazením. U klíčů nebo malých čipů lze zaměstnance dohledat pomocí jedinečného ID čipu nebo klíče, pokud ho evidujeme v nějakém systému, což však ale vyžaduje další prostředky.

4.1.4 Variabilita

Je nutné, aby bylo možné jednotlivým zaměstnancům přidávat a odebírat přístupová práva průběžně během doby vlastnictví jednoho identifikátoru. To lze velmi dobře provádět u všech identifikátorů, kde se uživatel ověřuje elektronicky, nikoli mechanicky. Zcela nám zde odpadají obyčejné i skupinové klíče. U nich lze změnu přístupových práv zaměstnance provést pouze přidáním/odebráním klíče.

4.1.5 Možnost dalšího využití identifikátoru

Cílem tohoto požadavku je umožnit provázání přístupových identifikátorů s dalšími firemními aplikacemi, jako například systém vedení docházky, obědy, přístup do

služebních vozidel. Toto lze velmi těžko s pomocí obyčejných nebo mechatronických identifikátorů. Zavádění otisku prstu bude nebo jiných biometrických metod určení uživatele by bylo značně nákladné.

4.1.6 Škálovatelnost

Přístupový systém bude budován postupně. Nejprve v Modelovém objektu, poté se bude postupně šířit dál po celém distribučním území. Je tedy potřeba, aby systém fungoval s jednou připojenou budovou nebo třeba několika desítkami a zvládal obsluhovat stovky až tisíce uživatelů. Zde se opět jeví velmi výhodně bezkontaktní karty, případně čipy. Jako nevhodné se jeví obyčejné i skupinové klíče, obzvlášť pokud někdo ze zaměstnanců má přístup do budov ve více městech.

4.1.7 Shrnutí

Jako ideální identifikační prostředek se na základě výše uvedených argumentů ukázaly čipové bezkontaktní karty. Nejen, že je lze pohodlně používat jako firemní průkaz, dokonce lze použít i ty stávající bez nutnosti výměny. Variabilita přiřazených práv je zajištěna tím, že ID uživatele je při každé žádosti o přístup vyhodnocováno na centrálním serveru, a tyto záznamy lze měnit i online bez přítomnosti fyzického nosiče (karty).

Výhodou je i možnost téměř neomezeného množství přístupových oblastí. Karty lze jednoduše zneplatnit „na dálku“, případně nastavovat jejich expiraci (pro návštěvníky). Další využití karet se přímo nabízí – docházkový systém, platby ve stravovacím zařízení nebo přístup ke sdíleným služebním vozidlům. Nakonec, samotný nosič (karta) je oproti ostatním docela levný.

4.2 Přístupový systém

Níže budou specifikovány prostředky přístupového systému jako podmnožiny technických opatření fyzické ochrany navržené pro jednotlivé typy objektů a některá organizační opatření (vztažená k použití konkrétních technických opatření).

4.2.1 Přístupový systém pro administrativní budovy

Administrativní budovy společnosti ENERGETIKA se nacházejí většinou v dobře dosažitelných částech (centrum) bývalých okresních měst. Většinou poskytují zázemí technikům správy, rozvoje a údržby sítě, obchodním zástupcům ze společnosti ENERGETIKA Prodej, a.s. a dalším administrativním pracovníkům důležitým pro chod

společnosti. V některých případech mohou obsahovat například i call centrum nebo datacentrum (v tom případě se pak musí řídit normami na zabezpečení KII).

Na rozdíl od ostatních typů budov je zde nutné počítat i se vstupem zákazníků, návštěvníků a jiných cizích osob.

4.2.1.1 Zabezpečení proti vniknutí osob

Opatření proti neoprávněnému vniknutí do budovy okny je provedeno bezpečnostní fólií nalepenou na zasklení oken. Veškeré dveře umožňující vstup do budovy musejí být v provedení bezpečností včetně zámkového kování. Veškeré možné stavební otvory umožňující proniknutí do chráněných budov (dveře, okna) musí být osazeny magnetickými kontakty. V místnostech jsou dále osazena pohybová čidla. Ve výjimečných případech mohou být instalována čidla detekující tříštění skla (pokud není mříž a pohybová čidla).

4.2.1.2 CCTV

Kamerový zabezpečovací systém se používá ve všech administrativních budovách. Kamerový systém je využíván ostrahou objektu pro dálkový dohled nad vstupy a vjezdy do areálu či jeho zón. Je-li kamerový systém instalován, musí být u vstupu do areálu i jinde na hranici chráněného perimetru čitelně uvedena informace, že je v areálu provozován kamerový systém. (33) (22)

Pevná kamera pouze s možností ostření, s přepínaným režimem Den/Noc se instaluje do míst, ze kterých je možné optimálně provádět dohled a automatický záznam situace u vchodu nebo vjezdu do areálu a rovněž na hranicích jednotlivých přístupových zón (tam, kde se osoba musí pro přístup identifikovat použitím bezkontaktní karty). Jsou primárně určeny pro automatický záznam vzniklých událostí, které jsou ve vizuálním dosahu dané kamerové sestavy. Kamery dle zákona nesmí být instalovány přímo na pracovišti, například v kanceláři. (33)

Pro ochranu vnějšího pláště budovy lze použít, pokud by Úřad pro ochranu osobních údajů instalaci kamer do těchto míst nepovolil, atrapy kamer a informační tabule, jako by se o kamery jednalo.

Výstupy všech kamer začleněných do PTZS musí být archivovány v definovaném archivačním zařízení pouze po stanovenou dobu (min. 7 dní). Archivace, používání

a zpřístupnění záznamů vybraným osobám musí být ve shodě s platnými zákonnými předpisy, především Zákonem o ochraně osobních údajů (22). Při zavádění systému CCTV lze postupovat dle *Metodiky pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* vydané Úřadem pro ochranu osobních údajů. (33)

4.2.1.3 Organizace vstupu do objektu

Hlavní vstup do budovy je opatřen recepcí, kde je v otevíracích hodinách (zpravidla od 6:00 do 18:00) přítomna fyzická ostraha objektu. Na recepci navazuje veřejně přístupná část objektu – poradenská místo, obchodní místo nebo prodejní kancelář. Do dalších částí areálu je vstup možný pouze s bezkontaktní kartou přes turniket. Zbytek areálu může být ještě dále rozdělen do zón podle různých kritérií (nejčastěji stavební dispozice, případně organizační struktura společnosti).

Zaměstnanec přichází do budovy přes hlavní vchod, v případě, že přichází před příchodem fyzické ostrahy, deaktivuje na terminálu poplachový systém. Prochází veřejnou částí a přes turniket pokračuje na své pracoviště. Cestou může procházet přes několik zabezpečených zón. Má-li do nich přístup, odemyká si je svojí bezkontaktní kartou. Při odchodu z areálu rozvodny zaměstnanec, který areál opustí jako poslední, provede aktivaci jednotlivých detekčních zón podle návodu k obsluze zabezpečovacího systému (obvykle přiložením karty ke čtečce na budově dvakrát za sebou). Aktivace a deaktivace detekčních zón musí mít optickou signalizaci. Vypnutí a zapnutí detekčních zón lze provádět i na dálku z dohledového pracoviště.

Čtečka bezkontaktních vstupních karet je umístěna na vjezdové bráně, na vstupním turniketu a dále pak u dalších dveří oddělující jednotlivé zóny v zabezpečených objektech. Informace o vstupech, stejně tak o neoprávněných pokusech o vstup (např. přiložení bezkontaktní karty neaktivované pro konkrétní objekt), jsou přenášeny na dohledové pracoviště, kde jsou archivovány.

V případě výpadku napájení čteček bezkontaktních karet může mít zaměstnanec přidělený vlastní bezpečnostní kód, kterým po vstupu do budovy (odemčení dveří pomocí příslušného zámkového systému) bez použití bezkontaktní karty deaktivuje PTZS zadáním kódu na ovládací klávesnici za vstupními dveřmi.

Při vstupu a odchodu z objektu, případně při vyvolání falešného poplachu, se zaměstnanec řídí pokyny uvedenými v místních provozních předpisech konkrétního areálu. V případě poplachového stavu se přenáší zpráva na dohledové pracoviště.

Systémy zabezpečení rozvodny jsou napojeny na dohledové pracovitě. Pokud dojde ke ztrátě spojení mezi střeženým objektem a dohledovým pracovištěm, nesmí dojít k deaktivaci jednotlivých systémů zabezpečení PZTS.

Všechny brány, branky, a vstupní dveře do jednotlivých zón areálu, které jsou zabezpečeny i pomocí PZTS, jsou vybaveny elektrickým zámkovým systémem. Zámky jsou prioritně ovládány systémem kontroly vstupů s definovaným oprávněním pro vstup osob a vjezd vozidel. Pro případ jakékoli poruchy, závady nebo nefunkčnosti elektrického ovládání zámků a ostatních elektromechanických pohonů a prvků pro vstupy do objektů musí být vždy zachována možnost ovládání zámků pomocí mechanických klíčů.

Odemknutí a otevření klíčem (nouzové použití klíče) je signalizováno formou poplachové zprávy a přenášeno na dohledové pracoviště. Všechny zámkové systémy musí minimálně splňovat požadavky bezpečnostní třídy č. 3 dle ČSN EN 1627.

Cizí osoby, které nemohou být odbaveny ve veřejné části areálu, dostávají dočasnou návštěvnickou bezkontaktní kartu, která je opravňuje přístupu do pouze konkrétní zóny areálu po omezený čas, a která je jasně identifikuje jako zákazníka.

4.2.2 Přístupový systém pro služebny

Služebny techniků a montérů distribuční sítě se na území, kde distribuci elektrické energie zajišťuje společnost ENERGETIKA, vyskytují většinou v obcích s rozšířenou působností. Jejich počet tedy zhruba odpovídá počtu těchto obcí. Služebny poskytují technickým pracovníkům zázemí (administrativa, hygiena), dále slouží k parkování služebních vozidel a také se v jejich objektech mohou nacházet menší sklady materiálu. Služebny mohou být součástí administrativních budov/center nebo rozvoden, v takovém případě přejímají zabezpečení těchto objektů.

Služebna je typicky areál s nějakou asfaltovou plochou, garážemi, sklady a budovou se zázemím pro techniky.

4.2.2.1 Zabezpečení proti vniknutí

Areál služebny musí být oplocen, vstupní branky a vjezdové brány musí být uzamykatelné. Elektrický pohon brány není nutnou podmínkou, stejně jako dálkové ovládání branky (pokud branka v areálu vůbec je). Garáže jsou vybaveny uzamykatelnými vraty.

Opatření proti neoprávněnému vniknutí do budovy okny je provedeno bezpečnostní fólií nalepenou na zasklení oken. Pro případ opakovaných pokusů o vniknutí do budovy budou okna opatřena dodatečně okenními mřížemi s povrchovou úpravou žárového zinkování. Veškeré dveře umožňující vstup do budovy musejí být v provedení bezpečností včetně zámkového kování. Veškeré možné stavební otvory umožňující proniknutí do chráněných budov (dveře, okna) musí být osazeny magnetickými kontakty. V místnostech jsou dále osazena pohybová čidla. Ve výjimečných případech mohou být instalována čidla detekující tříštění skla (pokud není mříž a pohybová čidla).

4.2.2.2 CCTV

Kamerový zabezpečovací systém se na služebnách používat nemusí, avšak v odůvodněných případech ho samozřejmě používat lze. Doporučuje se alespoň instalovat na některá místa atrapy kamer pro odstrašení případných zlodějů. I v takovém případě však musí být v areálu instalovány i informační tabulky upozorňující na přítomnost kamerového systému. (22)

Archivace, používání a zpřístupnění záznamů vybraným osobám musí být ve shodě s platnými zákonnými předpisy, především Zákonem o ochraně osobních údajů (22). Při zavádění systému CCTV lze postupovat dle *Metodiky pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* vydané Úřadem pro ochranu osobních údajů. (33)

4.2.2.3 Organizace vstupu do objektu

Při vjezdu do objektu pracovník odemkne vstupní bránu do areálu, opouští-li areál jako poslední, bránu za sebou zamyká. Jsou-li v areálu přítomni zaměstnanci společnosti ENERGETIKA, brána může být odemčené i otevřená. První příchozí po odemčení vstupu do objektu deaktivuje PTZS pomocí čipové karty nebo klávesnice (nebo kombinace) umístěné za vstupními dveřmi do objektu. Při odchodu z areálu služebny zaměstnanec, který areál opustí jako poslední, provede aktivaci jednotlivých detekčních zón podle

návodu k obsluze zabezpečovacího systému. Aktivace a deaktivace detekčních zón musí mít optickou signalizaci.

Systémy zabezpečení rozvodny jsou napojeny na dohledové pracovitě. Pokud dojde ke ztrátě spojení mezi střeženým objektem a dohledovým pracovištěm, nesmí dojít k deaktivaci jednotlivých systémů zabezpečení PZTS. V případě poplachového stavu se přenáší zpráva na dohledové pracoviště.

Cizí osoby, například dodavatelé služeb se v areálu mohou pohybovat pouze pod dohledem pověřeného pracovníka.

4.2.3 Přístupový systém pro rozvodny a elektrárny

Rozvodny se v distribuční síti společnosti ENERGETIKA nacházejí především u větších sídel, jejich počet už není tak veliký, jako u trafostanic, o to je ale jejich provoz kritičtější pro provoz celé sítě, čemuž musí odpovídat i režim přístupu do nich. Elektrárny jsou zvláštním případem, jejich počet je nevelký, režim přístupu je ale velmi podobný rozvodnám.

4.2.3.1 Zabezpečení proti vniknutí

Opatření proti neoprávněnému vniknutí do budovy okny je provedeno bezpečnostní fólií nalepenou na zasklení oken. Pro případ opakovaných pokusů o vniknutí do budovy budou okna opatřena dodatečně okenními mřížemi s povrchovou úpravou žárového zinkování. Veškeré dveře umožňující vstup do budovy musejí být v provedení bezpečností včetně zámkového kování. Veškeré možné stavební otvory umožňující proniknutí do chráněných budov (dveře, okna) musí být osazeny magnetickými kontakty. V místnostech jsou dále osazena pohybová čidla. Ve výjimečných případech mohou být instalována čidla detekující tříštění skla (pokud není mříž a pohybová čidla).

Vnější oplocení areálu musí být provedeno dle požadavků daných normami. Ty stanovují požadovanou výšku oplocení (2 m + 0,5 m ostnatý nebo žiletkový drát), parametry plotu, požadují vybavit oplocení i podhrabovými deskami, stejně jako definují požadavky na brány a branky. Detailnější informace lze nalézt v Příloze 1 a v Příloze 2 této práce.

4.2.3.2 CCTV

Kamerový zabezpečovací systém se používá pouze v rozvodnách se stálou obsluhou případně v objektech, kde je tento systém vyžadován charakterem provozu objektu.

Kamerový systém je využíván dohledovým pracovištěm pro dálkový dohled nad technologií rozvodny a vjezdem do rozvodny. Je-li kamerový systém instalován, musí být u vstupu do areálu i jinde na hranici chráněného perimetru čitelně uvedena informace, že je v areálu provozován kamerový systém. (33) (22)

Pevná kamera pouze s možností ostření, s přepínaným režimem Den/Noc se instaluje do míst, ze kterých je možné optimálně provádět dohled a automatický záznam situace u vjezdu do rozvodny a v technologické části rozvodny (zařízení primární techniky jako transformátor, vypínač atd.). Jsou primárně určeny pro automatický záznam vzniklých událostí, které jsou ve vizuálním dosahu dané kamerové sestavy.

Výstupy všech kamer začleněných do PTZS musí být archivovány v definovaném archivačním zařízení pouze po stanovenou dobu (min. 7 dní). Archivace, používání a zpřístupnění záznamů vybraným osobám musí být ve shodě s platnými zákonnými předpisy, především Zákonem o ochraně osobních údajů (22). Při zavádění systému CCTV lze postupovat dle *Metodiky pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů* vydané Úřadem pro ochranu osobních údajů. (33)

4.2.3.3 Organizace vstupu do objektu

Čtečka bezkontaktních vstupních karet je umístěna na vstupní bráně a dále pak na vnější zdi rozvodny nebo elektrárny vedle vchodových dveří a dalších zabezpečených objektech. Informace o vstupech, stejně tak o neoprávněných pokusech o vstup (např. přiložení bezkontaktní karty neaktivované pro konkrétní objekt), jsou přenášeny na dohledové pracoviště, kde jsou archivovány.

Při příchodu k budově zaměstnanec přiložením své bezkontaktní karty (s nastaveným oprávněním ke vstupu) ke čtečce provede deaktivaci jednotlivých detekčních zón. Při odchodu z areálu rozvodny zaměstnanec, který areál opustí jako poslední, provede aktivaci jednotlivých detekčních zón podle návodu k obsluze zabezpečovacího systému (obvykle přiložením karty ke čtečce na budově dvakrát za sebou). Aktivace a deaktivace detekčních zón musí mít optickou signalizaci. Vypnutí a zapnutí detekčních zón lze provádět i na dálku z dohledového pracoviště.

V případě výpadku napájení čteček bezkontaktních karet může mít zaměstnanec přidělený vlastní bezpečnostní kód, kterým po vstupu do budovy (odemčení dveří pomocí

příslušného zámkového systému) bez použití bezkontaktní karty deaktivuje PTZS zadáním kódu na ovládací klávesnici za vstupními dveřmi.

Při vstupu a odchodu z objektu, případně při vyvolání falešného poplachu, se zaměstnanec řídí pokyny uvedenými v místních provozních předpisech konkrétní rozvodny nebo elektrárny. V případě poplachového stavu se přenáší zpráva na dohledové pracoviště.

Ve vybraných objektech – uzlových rozvodnách se zřizuje vrátenská služba.

Systémy zabezpečení rozvodny jsou napojeny na dohledové pracovitě. Pokud dojde ke ztrátě spojení mezi střeženým objektem a dohledovým pracovištěm, nesmí dojít k deaktivaci jednotlivých systémů zabezpečení PZTS.

Všechny brány, branky, vstupní dveře do skladů a dalších objektů rozvodny, které jsou zabezpečeny i pomocí PZTS, jsou vybaveny elektrickým zámkovým systémem. Zámky jsou prioritně ovládány systémem kontroly vstupů s definovaným oprávněním pro vstup osob a vjezd vozidel. Pro případ jakékoli poruchy, závady nebo nefunkčnosti elektrického ovládání zámků a ostatních elektromechanických pohonů a prvků pro vstupy do objektů musí být vždy zachována možnost ovládání zámků pomocí mechanických klíčů.

Odemknutí a otevření klíčem (nouzové použití klíče) je signalizováno formou poplachové zprávy a přenášeno na dohledové pracoviště. Všechny zámkové systémy musí minimálně splňovat požadavky bezpečnostní třídy č. 3 dle ČSN EN 1627.

Cizí osoby, například dodavatelé služeb se v areálu mohou pohybovat pouze pod dohledem pověřeného pracovníka.

4.2.4 Přístupový systém pro trafostanice

Trafostanic v distribuční síti společnosti ENERGETIKA je značné množství. V městech bychom je mohli počítat po desítkách, v těch nejmenších vesnicích musí být alespoň jedna. Samostatnou kapitolou pak jsou větší odběratelé elektřiny (nákupní centra, výrobní závody a další). Některé trafostanice se starají třeba jen o napájení jedné konkrétní ulice.

4.2.4.1 Zabezpečení proti vniknutí

Veškeré dveře nebo umožňující vstup do budovy musejí být v provedení bezpečností včetně zámkového kování. Vrata musí být vybavena zámkem a splňovat požadavky

uvedené v bodu 10 Přílohy 2, tohoto dokumentu, stejně jako zabezpečení případných oken. Nemá-li trafostanice plášťovou ochranu, tedy jedná se o venkovní trafostanici umístěnou na sloupu nebo sloupech, jedná se o ochranu polohou. V takovém případě musí být zařízení umístěno tak, aby nebylo bez použití dalších prostředků dosažitelné.

4.2.4.2 CCTV

Trafostanice nejsou vybaveny kamerovým systémem.

4.2.4.3 Organizace vstupu do objektu

Přístup do trafostanice je možný odemčením zámku vstupních vrat nebo dveří pomocí skupinového klíče. Po provedení všech požadovaných úkonů při opouštění objektu opět trafostanici zamkne. Trafostanice nesmí být uzamčena, je-li uvnitř přítomen člověk. Technik distribuční soustavy se tak jedním klíčem dostane do všech trafostanic v jím spravované oblasti.

Cizí osoby, například dodavatelé služeb se v areálu mohou pohybovat pouze pod dohledem pověřeného pracovníka při vypnutém zařízení.

4.2.5 Přístupový systém pro venkovní a kabelové vedení

Venkovní a kabelové vedení se vyskytuje prakticky všude, kde si vzpomeneme a je k němu zdánlivě snadný přístup. Samotné vedení jako takové je před nežádoucími lidskými zásahy chráněno svojí polohou – bez speciálního vybavení (žebřík, vysokozdvižná plošina) je pro člověka nedosažitelné. Kabelové vývody ze země ústí přímo do trafostanic, případně jsou vyvedeny ještě izolované až na vršek sloupu elektrického vedení. Více se ochranou vedení nebudeme zabývat.

4.2.6 Přístupový systém pro rekreační objekty

Skupina ENERGETIKA vlastní několik rekreačních objektů rozesetých na různých místech České republiky. I k nim je potřeba nějakým způsobem řídit přístup. Často se jedná o běžné chaty, někdy se zahradou, terasou, hřištěm či bazénem, lokalizované buď v obci, nebo mimo ni.

4.2.6.1 Zabezpečení proti vniknutí

Rekreační objekty jsou vybaveny běžnými dveřmi s normálním a bezpečnostním zámkem, běžnými okny. Na rekreačních zařízeních je instalován alarm, který je aktivován v době, kdy je zařízení opuštěno. Alarm aktivuje správce zařízení.

4.2.6.2 CCTV

Rekreační zařízení nejsou vybavena kamerovým systémem.

4.2.6.3 Organizace vstupu do objektu

Rekreantovi jsou vydány klíče od objektu správcem na základě platného poukazu vydaného příslušným oddělením společnosti ENERGETIKA ČR, s.r.o. Rekreant je seznámen s provozním řádem a bezpečnostními pokyny. Na konci pobytu rekreant předá objekt a klíče zpět správci v původním stavu.

4.3 Režimová opatření

Režimová opatření předepisují dodržování určitých určité postupů k správnému fungování přístupového systému s výše zmíněnými technickými prostředky. Režimová opatření k řízení přístupu vychází především z příloh A9 a A11 normy ČSN ISO/IEC 27001:2014. (8)

4.3.1 Požadavky organizace na řízení přístupu

4.3.1.1 Politika řízení přístupu

Politika řízení přístupu musí být ustavena, dokumentována a přezkoumávána v závislosti na požadavcích na činnosti organizace a bezpečnosti informací. (8)

4.3.1.2 Přístup k aktivům

Uživatelé musí mít přístup pouze k těm aktivům, pro jejich použití byli zvlášť oprávněni. K ostatním aktivům mají přístup zakázán. (8)

4.3.2 Řízení přístupu uživatelů

4.3.2.1 Registrace a zrušení registrace uživatele

„Při přidělování přístupových práv musí být implementován proces formalizované registrace uživatele včetně jejího zrušení.“ (8) To se týká nejen zaměstnanců při jejich přijímání a přidělování přístupových práv, ale cizích osob, kterým jsou vydávány návštěvnické karty. O cizí osobě je při vydání návštěvnické karty nutné zpracovávat osobní údaje (jméno, bydliště, číslo OP, účel návštěvy), zároveň je nutné tyto osoby alespoň nějakým základním způsobem proškolit v oblasti provozního řádu budovy (bezpečnostní zóny, zakázané chování, evakuace atd.).

4.3.2.2 Správa uživatelských přístupů

„Pro přidělování a odebírání přístupových práv všem typům uživatelů ke všem aktivům musí být implementován formalizovaný proces správy uživatelských přístupů.“ (8) Tento bod se týká i nastavení pravidel říkajících, kdo smí komu vydávat oprávnění k přístupu ke kterým aktivům a na jak dlouho. Jako příklad lze uvést vydávání návštěvnických karet s omezenou působností i časovou platností pracovníkem fyzické ostrahy.

4.3.2.3 Správa privilegovaných přístupových práv

„Musí být omezeno a řízeno přidělování a používání privilegovaných přístupových práv.“ (8) Například není možné, aby pracovník zodpovědný za centrální přidělování přístupových práv umožnil toto činit ještě někomu dalšímu, kdo k tomu nebyl původně určen.

4.3.2.4 Správa tajných autentizačních informací uživatelů

„Přidělování tajných autentizačních informací musí být řízeno formalizovaným procesem.“ (8) Mělo by tedy být popsáno, jakým způsobem bude zaměstnanci například sdělen kód pro deaktivaci PTZS.

4.3.2.5 Přezkoumání přístupových práv uživatelů

„Vlastníci aktiv musí v pravidelných intervalech přezkoumávat přístupová práva uživatelů.“ (8) Přezkoumávání přístupových práv by mělo probíhat ve vhodně nastaveném časovém intervalu (například 1 rok) a navíc pokaždé, dojde-li k nějaké změně statutu zaměstnance – změna pracovního poměru, zařazení na jinou pracovní pozici, stěhování se v rámci objektu atd.

4.3.2.6 Odebrání nebo úprava přístupových práv

„Při ukončení nebo změně pracovního vztahu, smluvního vztahu nebo dohody musí být všem zaměstnancům a externím stranám odejmuta nebo pozměněna přístupová práva k aktivům.“ (8) Tento proces by měl v ideálním případě probíhat tak, že budou nejprve subjektu všechna práva odejmuta a na základě odůvodněné potřeby případně přiznána nová nebo znovu ta původní.

4.3.3 Odpovědnosti uživatelů

4.3.3.1 Používání tajných autentizačních informací

„Při používání tajných autentizačních informací musí být po uživatelích vyžadováno, aby dodržovali postupy stanovené organizací.“ (8) Můžeme po zaměstnancích například požadovat, aby nikde nesdělovali tajné informace (PIN kódy pro aktivaci/deaktivaci PZTS), případně je patřičně chránili před zneužitím cizí osobou.

4.3.4 Bezpečné oblasti

Cílem je předcházet neautorizovanému fyzickému přístupu, poškození a zásahům do informací a vybavení organizace

4.3.4.1 Fyzický bezpečnostní perimetr

Bezpečnostní perimetry musí být definovány a používány k ochraně oblastí, které obsahují důležitá nebo kritická aktiva. (8)

4.3.4.2 Fyzické kontroly vstupu¨

„Aby bylo zajištěno, že je přístup do bezpečných oblastí povolen pouze oprávněným osobám, musí být tyto oblasti chráněny vhodným systémem vstupních kontrol.“ (8) Toho se snaží dosáhnout zde navrhovaný přístupový systém.

4.3.4.3 Zabezpečení kanceláří, místností a vybavení

„Musí být navržena a aplikována fyzická bezpečnost kanceláří, místností a vybavení.“ (8) Každá osoba bude mít přidělena oprávnění pouze do určité množiny místností a kanceláří. Ať už pomocí bezkontaktních karet, tak běžných (skupinových) klíčů.

4.3.4.4 Ochrana před vnějšími hrozbami a hrozbami prostředí

„Musí být navržena a aplikována fyzická ochrana proti přírodním katastrofám, úmyslnému útoku nebo haváriím.“ (8)

4.3.4.5 Práce v bezpečných oblastech

„Musí být navrženy a aplikovány postupy pro práci v bezpečných oblastech.“ (8)

4.3.4.6 Oblasti pro vykládku a nakládku

Přístupové body, jako oblasti pro nakládku a vykládku a další místa, kde se mohou neoprávněné osoby dostat do prostor organizace, musí být kontrolovány. (8)

4.3.5 Zařízení

Cílem je předcházet ztrátě, poškození, krádeži nebo kompromitaci aktiv a přerušení činnosti organizace.

4.3.5.1 Umístění zařízení a jeho ochrana

„Zařízení musí být umístěna a chráněna tak, aby se snížila rizika hrozeb a nebezpečí daná prostředím a aby se omezily příležitosti pro neoprávněný přístup.“ (8) Dobrým příkladem realizace tohoto opatření je například umístění kamer CCTV mimo běžný dosah člověka.

4.3.5.2 Podpůrné služby

„Zařízení je chráněno před selháním napájení a před dalšími výpadky způsobenými selháním podpůrných služeb.“ (8) Přístupový systém musí obsahovat některé redundantní prvky. Jednak záložní napájení, aby byla zajištěna možnost pohybu osob po budově i v případě výpadku elektřiny, také to ale musí být redundance serveru řídicího přístupový systém nejlépe ve stejné budově, kdyby došlo k výpadku spojení s centrálním serverem.

4.3.5.3 Bezpečnost kabelových rozvodů

„Silové a telekomunikační kabelové rozvody, které jsou určeny pro přenos dat nebo podporu informačních služeb, musí být chráněny před odposlechem, rušením či poškozením.“ (8)

4.3.5.4 Údržba zařízení

„Zařízení musí být správně udržováno pro zajištění jeho stálé dostupnosti a integrity.“ (8)

4.3.5.5 Uživatelská zařízení bez obsluhy

„Uživatelé musí zajistit přiměřenou ochranu zařízení bez obsluhy.“ (8) Toto opatření lze vztáhnout například na opouštění budov – nutnost aktivovat detekční zóny PTZS, nebo i prosté zavírání dveří oddělujících jednotlivé přístupové zóny objektu.

4.4 Dotčené osoby

Změnou přístupového systému budou dotčeny všechny osoby, které mají se skupinou ENERGETIKA takový vztah, že potřebují vstupovat do jejích objektů a areálů.

Primárně se změna bude dotýkat všech zaměstnanců při výkonu každodenní pracovní činnosti. Mimo to se bude přímo dotýkat i některých zákazníků, návštěvníků nebo dodavatelů, kteří budou při pohybu po objektech společnosti ENERGETIKA nuceni používat prostředky přístupového systému. O všech uživatelích budou shromažďována určitá osobní data (místo a čas, kamerové záznamy).

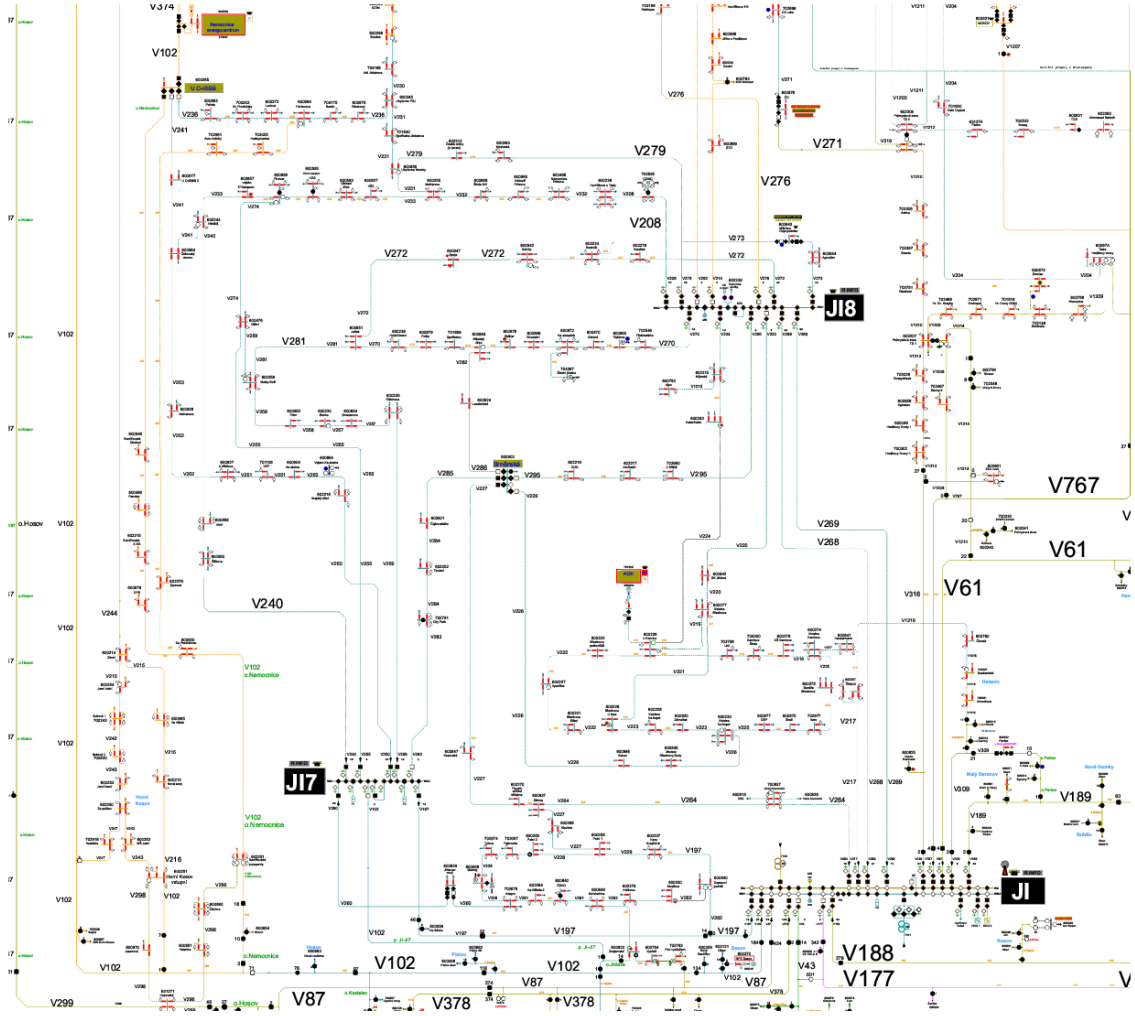
Vydávání dočasných přístupových karet a shromažďování osobních údajů mimořádně dopadne na externí pracovníky fyzické ostrahy, kterým tak přibude nová povinnost a zároveň nutnost naučit se dovednosti potřebné k vydávání karet.

4.5 Modelový objekt

Modelový objekt se nachází v bývalém okresním, dnes krajském městě. Sdružuje v sobě několik funkcí – obchodní kancelář pro styk s koncovým zákazníkem (ENERGETIKA Prodej, a.s.), služebnu (zázemí pro techniky ENERGETIKA Servis, s.r.o.), rozvodnu 22/22 kV (ENERGETIKA Distribuce, a.s.) a zázemí pro regionální projektanty a další (ENERGETIKA ČR, s.r.o.). Jedná se tedy o velmi komplexní objekt, kde se mohou pohybovat zaměstnanci celkem 4 společností ze skupiny ENERGETIKA, externí dodavatelé (ostraha), návštěvníci a zákazníci. Mimo to se v objektu nachází dvůr se stáními pro služební vozidla a garáže pro některá speciální vozidla. Dispozice Modelového objektu je zobrazena na leteckém snímku na Obr. 9.

Obr. 9: Letecký 3 D pohled na Modelový objekt. Zdroj: www.mapy.cz

Rozvodna v modelovém objektu je typu 22/22 kV a zásobuje elektrickou energií celé město včetně nemocnice a několik okolních obcí, odhadem přes 50 tisíc obyvatel (viz Obr. 10), je tedy žádoucí k rozvodně přistupovat jako k prvku kritické infrastruktury.



Obr. 10: Schéma distribuční soustavy v okolí rozvodny 22/22 kV v Modelovém objektu. Zdroj: ENERGETIKA Distribuce, a.s.

V modelovém objektu, jak již bylo zmíněno výše, se pohybují zaměstnanci různých společností v rámci holdingu ENERGETIKA. Tabulka Tab. 3 ukazuje výčet rolí pracovníků v rámci Modelového objektu a jejich přibližné počty.

Pracovní zařazení	Počet osob
Ostraha	1
Obchodníci	2
Správci nemovitostí	2

Pracovní zařazení	Počet osob
Vedoucí a asistentka vedoucího RCDS	1+1
Vedoucí řízení výstavby	1
Technik výstavby, rozvoje a obnovy DS	3
Technici správy sítě, technici provozu a údržby	4+2
Technik dokumentace VN a NN	1
Technik provozu a zakázek	1
Technici provozu a údržby rozvoden	4
Montéři distribuční soustavy, koordinátor OPDS	7+1
Koordinátor, technik a montéři práce pod napětím	1+1+3
Technici měřícího vozu	2

Tab. 3: Pracovní zařazení zaměstnanců v Modelovém objektu. Zdroj: Vlastní

Přehledová tabulka obsahující soupis všech místností v modelovém objektu je obsažena v Příloze 9 této práce.

Cílem nových opatření bude rozdělit pracovníky v objektech tak, aby se co nejvíce zkrátili vzdálenosti mezi těmi, kdo spolu potřebují komunikovat nejčastěji, případně aby návštěvníkovi přicházejícímu s konkrétní žádostí stačilo umožnit přístup do jedné konkrétní zóny objektu.

4.5.1 CCTV

Do areálu Modelového objektu lze vstoupit třemi možnými vstupy. Prvním je hlavní vstup s recepcí a stanovištěm ostrahy do objektu v plánech označeného jako *budova dopravy*. Druhým je samostatný vstup do objektu služebny. Třetím vstupem do areálu je vjezdová brána a branka do dvora areálu. Ze dvora areálu lze vstupovat do všech tří budov, tedy do *budovy dopravy*, *služebny* i *rozvodny*. Rozvodna tedy není přímo přístupná z ulice. Od vnějšího okolí je areál Modelového objektu oddělen částečně vnějším pláštěm budov a částečně zdí. Všechny tři vstupy do areálu Modelového objektu jsou monitorovány pomocí systému CCTV, stejně jako všechny vstupy do jednotlivých objektů ze dvora.

Na hranici areálu Modelového objektu a veřejného prostranství (ne do vnitrobloku), tedy na obvodových zdech budov a obvodové zdi dvora jsou instalovány makety kamer CCTV pro alespoň částečné odstrašení případného útočníka. Instalovat do těchto míst kamery se

záznamem je dle Zákona o ochraně osobních údajů jen těžko odůvodnitelné, neboť se jedná o veřejné prostranství (chodník) a nejsou zde žádné vstupy do areálu.

Kamerový systém je instalován i ve vnitřních prostorách všude tam, kde zaměstnanci nebo návštěvníci prochází přes zařízení přístupového systému – turnikety, dveře otevírané bezkontaktními kartami. Jedná se hlavně o chodby uvnitř objektů.

4.5.2 Přístupový systém

Areál Modelového objektu se skládá ze tří budov a vnitřního dvora. Žádná z částí Modelového objektu není plně veřejně přístupná v libovolnou denní dobu. Přehledová tabulka obsahující soupis všech místností v modelovém objektu je obsažena v Příloze 9 této práce. Rozmístění budov v modelovém objektu a instalaci kamer CCTV ve venkovních prostorách je znázorněno na Obr. 11.

	Režim vstupu		**Režim pohybu osob**
	Vstup na kartu (turniket)		Volný vstup v provozní době budovy
	Vstup na kartu (dveře)		Volný vstup v otevírací době obchodní kanceláře
	Vstup do trafostanice		Přístupné s návštěvnickou kartou
	Vstup do rozvodny		Rozvodna

Tab. 4: Legenda k plánům

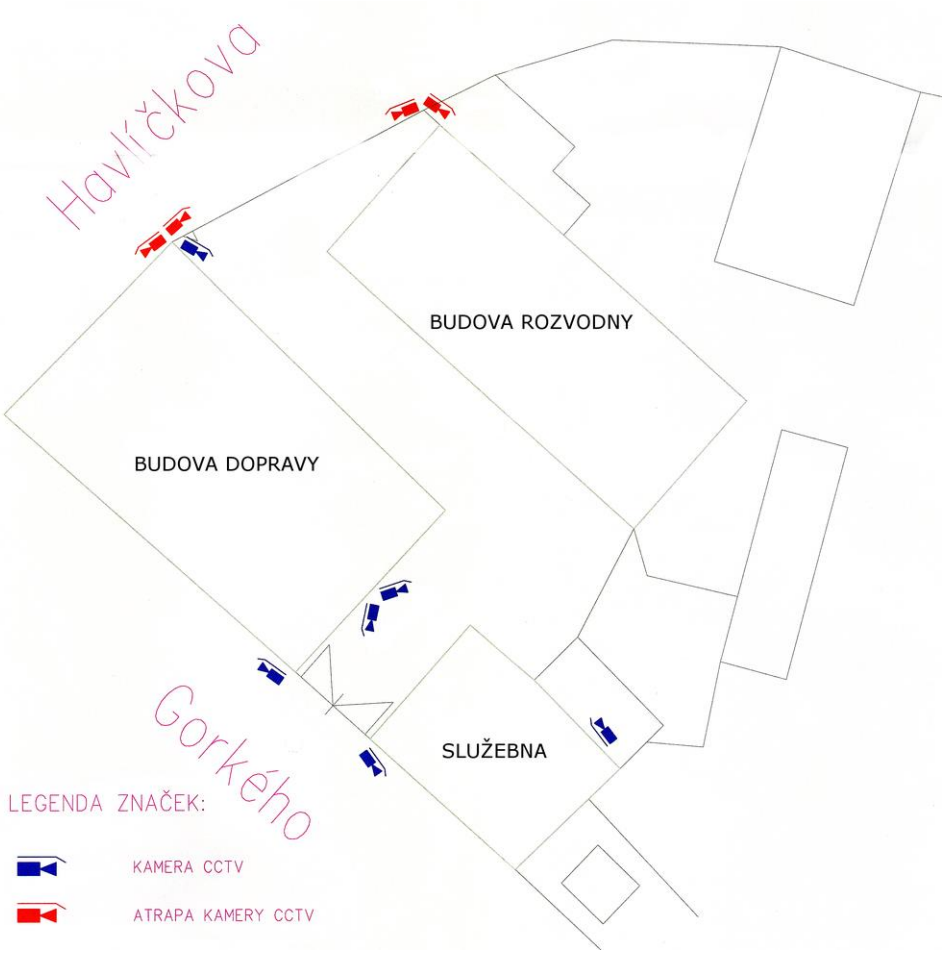
4.5.2.1 Dvůr

Vnitřní Dvůr je přístupný vjezdovou branou a brankou z veřejné komunikace a dále ze všech budov v areálu modelového objektu. Vjezdová brána má elektrický pohon a otevírá se pomocí bezkontaktní karty zaměstnance, případně ji může otevřít pracovník ostrahy z recepce, například pro vjezd vozidel některých dodavatelů. Vstup z budov je umožněn dveřmi, které se otevírají bezkontaktní kartou (oboustranně). Jako únikový východ slouží branka vedle vjezdové brány, kterou lze zevnitř dvora odemknout tlačítkem umístěným na plášti budovy dopravy.

Z vnitřního Dvora jsou přístupné garáže a sklady v budově služebny a vchody do všech tří budov. Na Dvoře se nachází několik krytých a několik nekrytých stání pro služební vozidla.

Na dvůr mají přístup všichni zaměstnanci a někteří návštěvníci, kteří míří za techniky do budovy rozvodny.

Dvůr je střežen kamerami systému CCTV, jejich rozmístění je znázorněno na Obr. 11.



Obr. 11: Situace areálu, CCTV. Zdroj: Vlastní

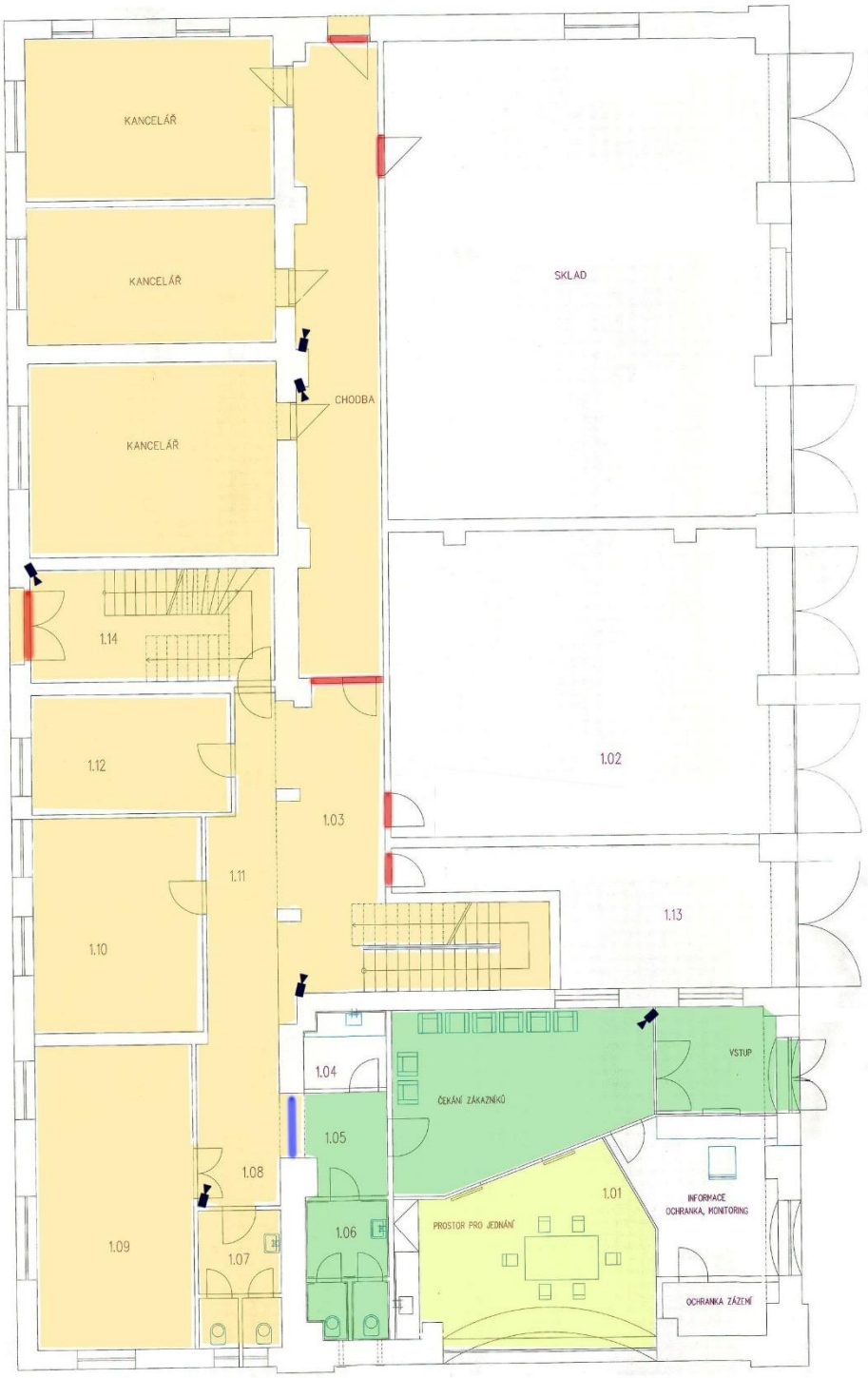
4.5.2.2 Budova dopravy

Vstupní objekt celého areálu Modelového objektu. V 1. nadzemním podlaží (1NP) se nachází hlavní vstup do budovy, za nímž je recepce – stanoviště ochranky a prostor pro čekání zákazníků (zde jsou k dispozici nejčastěji používané formuláře a další materiály). Sem má veškerá veřejnost přístup kdykoli v otevíracích hodinách budovy (všední dny

6:00 – 18:00, když je přítomna ostraha). Dále je veřejnosti v určitých provozních hodinách přístupná obchodní kancelář (místnost 1.01). Čekajícím zákazníkům jsou k dispozici toalety.

Přístup dále do objektu je možný pouze pomocí bezkontaktní karty s oprávněním k přístupu do příslušných prostor. Mezi místnostmi 1.05 a 1.08 je umístěn turniket, na jehož správné používání dohlíží kamera CCTV.

Na chodbu 1.08 přímo navazuje chodba 1.11 a 1.03 se schodištěm do 2NP a schodiště 1.14 do 1PP. Pro vstup do chodby „CHODBA“ je nutné použití bezkontaktní karty, stejně jako pro vstup do garáží 1.13 a 1.02. Kanceláře 1.09, 1.10 a 1.12 jsou již přístupné bez karty.



Obr. 12: Budova dopravy, 1NP. Zdroj: Vlastní

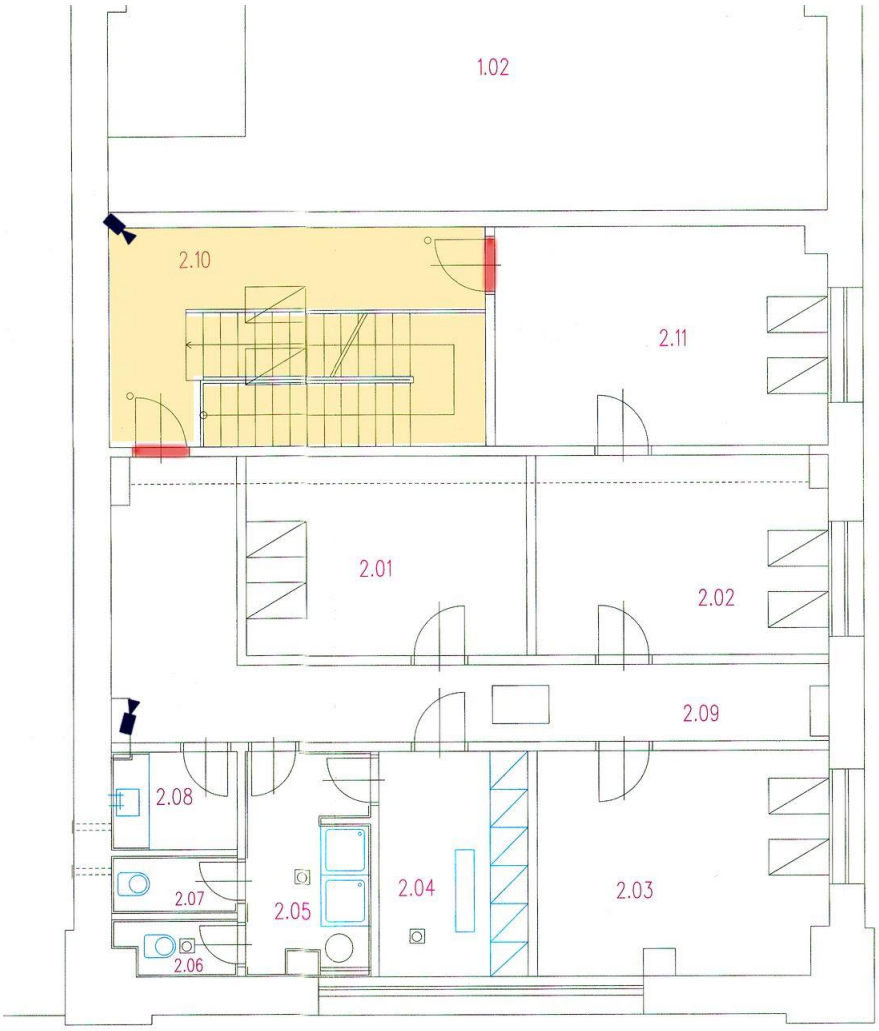
Do chodby „CHODBA“ je vstup možný pomocí bezkontaktní karty ze Dvora, z chodby 1.03 nebo ze skladu „SKLAD“. Z chodby „CHODBA“ jsou již přímo přístupné 3 kanceláře. Pro vstup do skladu „SKLAD“ je nutné použít bezkontaktní kartu.

Z chodby 1.14 je možný východ na Dvůr (s bezkontaktní kartou) a po schodišti přístup do suterénu.

Obr. 13: Budova dopravy, 1PP. Zdroj: Vlastní

V 1. podzemním podlaží (1PP) je ze schodiště 1.14 volně přístupná úklidová komora 0.06. S bezkontaktní kartou je pak přístup umožněn do místnosti 0.05 (v plánech vedeno jako archiv) a na ni navazujících sociálních zařízení 0.01 až 0.04. Vstup do místnosti 0.05 je z chodby střežen kamerou CCTV.

Ve 2. nadzemním podlaží (2NP) budovy dopravy schodiště z chodby 1.03 pokračuje jako chodba 2.10. Z chodby 2.10 je s pomocí bezkontaktní karty přístupná průchozí kancelář montérů PPN 2.11, tyto dveře jsou střeženy kamerou CCTV z chodby. Na druhé straně je s bezkontaktní kartou přístupný také vstup do chodby 2.09. Z chodby 2.09 se lze volně dostat do kanceláří a sociálních zařízení, s bezkontaktní kartou zpět na schodiště 2.10. Dveře mezi chodbami 2.09 a 2.10 jsou pomocí CCTV střeženy z obou stran.



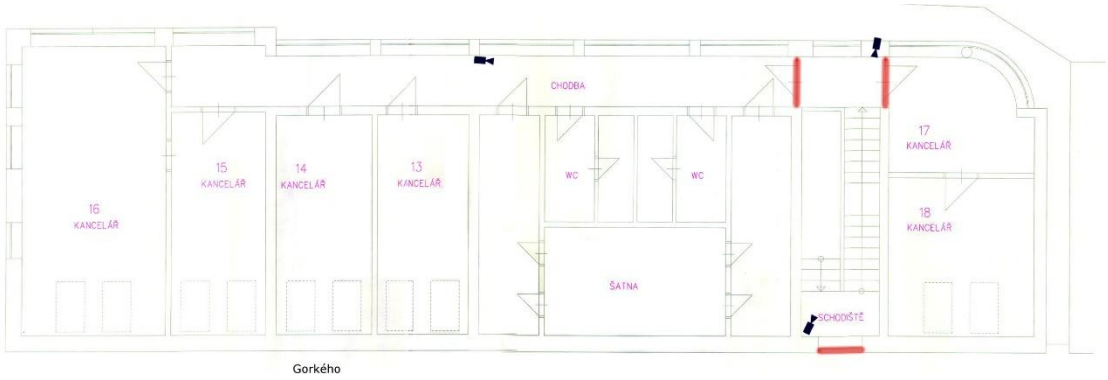
Obr. 14: Budova dopravy, 2NP. Zdroj: Vlastní.

4.5.2.3 Služebna (nová budova)

Do budovy Služebny ústí dva vchody. Jeden z veřejné komunikace, druhý ze dvora. Oba vchody ústí na schodiště, které je spojuje navzájem a umožňuje přístup do horního patra budovy. Přístup na schodiště i východ z něj je možný pouze s bezkontaktní kartou. Zaměstnanci, kteří pracují v této budově tak nemusí chodit přes hlavní vstup – recepci.

V 1. nadzemním podlaží (1NP) jsou kanceláře montérů, šatna a sociální zařízení. Kanceláře 17 a 18 jsou přímo přístupná ze schodiště „SCHODIŠTĚ“ pomocí bezkontaktní karty. Ostatní kanceláře, šatna a sociální zařízení jsou přístupné z chodby „CHODBA“, na niž se dá ze schodiště dostat pouze s bezkontaktní kartou. Všechny průchody jsou střeženy i kamerovým systémem CCTV oboustranně, kromě vstupu do kanceláře 17, ten je střežen pouze ze strany z chodby.

Ve spodním podlaží služebny se nachází tři garáže a dva sklady přístupné ze dvora. Vstup do nich je střežen kamerovým systémem CCTV z vnější strany. Bezkontaktní karty se zde nepoužívají.



Obr. 15: Služebna, 1NP. Zdroj: Vlastní.

Veřejnost do budovy Služebna nemá přístup. Výjimkou jsou pracovníci dodavatelských firem po dobu práce na zakázce (například stavební úpravy nebo opravy budovy).

4.5.2.4 Budova rozvodny

Budova rozvodny sloužila v minulosti pouze jako rozvodna, později ale částečně byla částečně přestavěna na kanceláře.

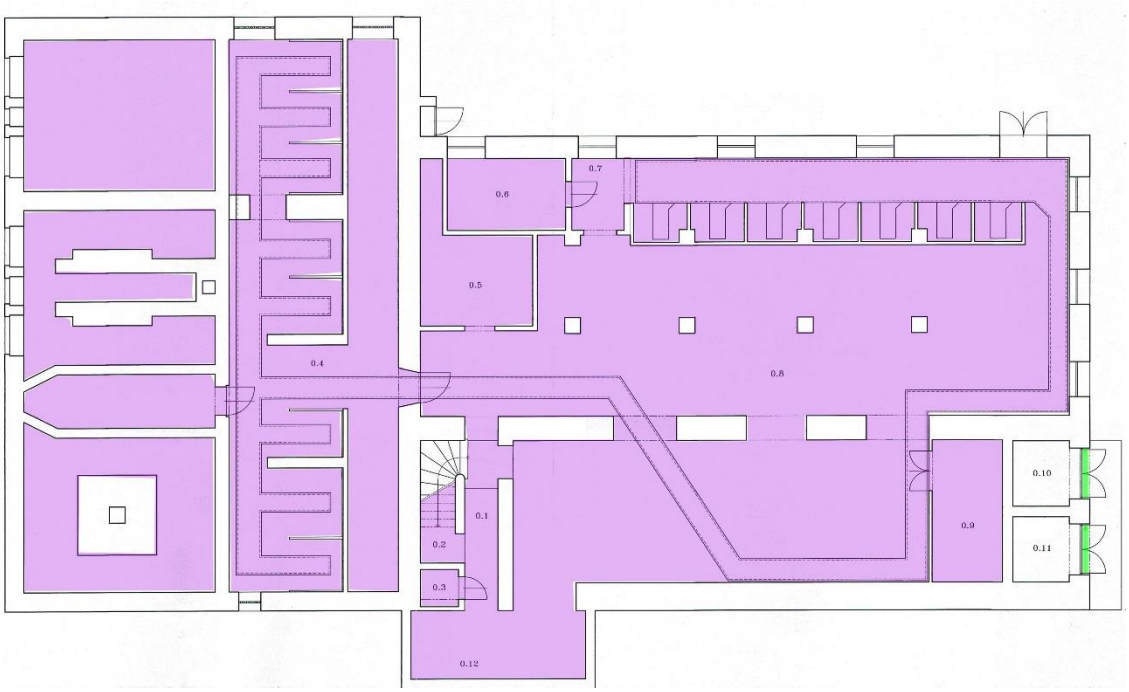
Obr. 16: Rozvodna, 1NP. Zdroj: Vlastní.

Do budovy ústí několik vstupů, všechny ze Dvora. Budeme-li v plánu budovy postupovat zprava, prvním vstupem je vstup do místnosti 1.9 (rozvaděč NN k vlastní trafostanici).

V podstatě se jedná o trafostanici, k níž mají přístup pracovníci společnosti ENERGETIKA Distribuce, a.s. za účelem údržby, revizí a oprav stejně jako k jakékoli jiné trafostanici, tedy pomocí skupinového klíče.

Další je vstup do chodby 1.14, která zpřístupňuje dvě kanceláře 1.10 a 1.11 a sociální zařízení. Tento vstup je možný pouze s bezkontaktní kartou. Tyto kanceláře se momentálně nevyužívají.

Přes dispečink rozvodny 1.15 je možný přístup do rozvodných sálů rozvodny VN (22/22 kV, místnosti 1.8 a 1.3). Vstup do těchto prostor se řídí režimem vstupu do rozvodny (viz kapitola 4.2.3.3). Veřejnost do těchto prostor není oprávněna vstupovat. Jedná se o prvek KI.



Obr. 17: Rozvodna, 1PP. Zdroj: Vlastní.

Vstup 1.1 umožňuje přístup do kanceláře 1.16 (momentálně využívané jako archiv) a dále na schodiště spojující 1. nadzemní podlaží s podkrovím (2NP) a suterénem (1PP). Schodiště 0.2 vedoucí do suterénu vede do rozvodných sálů rozvodny VN, proto je třeba vstup na něj řídit v režimu vstupu do rozvodny. Kromě toho umožňuje přímý přístup do rozvodných sálů 1.3 a 1.8. Vstup do těchto prostor se řídí režimem vstupu do rozvodny. Místnost 1.11 je sledována systémem CCTV.

Poslední vstup zpřístupňuje ze Dvora nově vybudované kanceláře 1.4, 1.5, 1.6 a 1.7. Tento vstup je opatřen zařízením čtecím bezkontaktní karty a ze Dvora sledován kamerou CCTV.

V suterénu budovy rozvodny se nachází 2 trafostanice (místnosti 0.10 a 0.11) přístupné ze Dvora v režimu přístupu k trafostanicím, tedy pomocí skupinového klíče. Zbytek suterénu je zařízení rozvodny VN (prvek KI). Přístup sem je možný pouze po zabezpečeném schodišti 0.2 z 1NP.

Obr. 18: Rozvodna, 2NP. Zdroj: Vlastní

V podkroví budovy rozvodny (2NP) se nachází kanceláře, zasedací místnosti a sociální zařízení. Schodiště z 1NP ústí na chodbu 2.01, z té jsou volně přístupné toalety, kuchyňka a úklidová místnost. Kanceláře a zasedací místnosti jsou pak přístupné z chodeb 2.07 a 2.19. Pro vstup na chodbu 2.07 nebo 2.19 z chodby 2.01 (a zpět) je nutné použít bezkontaktní kartu. Oboje tyto dveře jsou z obou stran sledovány kamerami CCTV se záznamem.

4.5.3 Pravidla přístupu

Do objektu rozvodny VN (suterén budovy rozvodny, rozvodné sály v přízemí a dispečink rozvodny) mají přístup jen pověření zaměstnanci společnosti ENERGETIKA Distribuce, a.s. Veškeré pokusy o přístup (úspěšné i neúspěšné) jsou zaznamenávány.

Do objektu Služebny mají přístup pouze pracovníci příslušných útvarů (montéři), správci budov, ostraha a pověření dodavatelé stavebních a jiných prací.

Do běžných kanceláří k technikům správy, údržby a rozvoje sítě je přístup veřejnosti možný, stejně jako k manažerům a obchodníkům. Vstup návštěvy dále do objektu probíhá následovně:

1) Návštěvník se přihlásí u ostrahy na recepci, sdělí ostraze své osobní údaje a účel návštěvy.
2) Ostraha předá návštěvníkovi formulář souhlasu se zpracováním osobních údajů a stručný provozní řád budovy, s nímž se návštěvník musí seznámit a toto seznámení podpisem stvrdit.
3) Mezi tím ostraha kontaktuje příslušného zaměstnance, za nímž návštěvník míří.
4) Souhlasí-li zaměstnanec, předá ostraha návštěvníkovi návštěvnickou kartu a instrukce, kudy se má vydat, případně vyzve zaměstnance, aby si návštěvníka vyzvedl na recepci.
5) Návštěvnická karta opravňuje návštěvníka ke vstupu pouze do prostor nezbytných k dosažení jeho cíle a neumožňuje opustit budovu jiným než hlavním vchodem.
6) Při odchodu návštěvník vrací kartu a ostraha o tom vede záznam.
7) Pro případ odcizení karty je její platnost omezena vždy jen na několik hodin. Pro další použití musí být znovu ostrahou aktivována.
8) Při opakované návštěvě již návštěvník nemusí být proškolen s provozním řádem budovy a rovněž nemusí podepisovat souhlas se zpracováním osobních údajů, pokud ho před tím neodvolal. (Odvolat souhlas se zpracováním osobních údajů lze dle Zákona o ochraně osobních údajů i nařízení GDPR (22) (23)).
9) Častí návštěvníci či dodavatelé mohou mít přiděleny své vlastní karty (u častých návštěvníků nutné vždy alespoň aktivovat, u dodavatelů například platnost po dobu konání prací).
10) Zaměstnanci cizích útvarů sídlící mimo Modelový objekt mohou mít automaticky přístup do některých částí objektu (nadřízení), případně si musí o přístup požádat stejně jako návštěvy (například technici z jiných měst).

Do obchodní kanceláře je v jejích úředních hodinách vstup veřejnosti volný.

Vjezd na Dvůr je povolen pouze služebním vozidlům případně soukromým vozidlům zaměstnanců schválených pro služební cesty. Pro parkování soukromých vozidel zaměstnanců slouží parkoviště před budovou Služebny přístupné z veřejné komunikace.

Přístupová práva do jednotlivých zón jsou jednotlivým zaměstnancům nastavena podle jejich pracovního zařazení a náplně a jsou pravidelně revidována. Navíc jsou revidována vždy, když dojde ke změně pracovního zařazení zaměstnance. (viz kapitola 4.3.2.5) Přístupová práva přiděluje přímý nadřízený zaměstnance.

Jednotlivé kanceláře mají ve dveřích běžný zámek s cylindrickou vložkou, zaměstnanci si je v době nepřítomnosti zamykají. Správci budov a ostraha mají pro případ potřeby k dispozici generální klíč.

4.5.4 Zvládání nestandardních stavů

Jelikož je přístupový systém v budově plně elektronický, je jeho provoz kriticky závislý na připojení zdroje elektrické energie. V případě výpadku proudu by mohlo hrozit uvěznění osob v budově. Proto je nutné, aby přístupový systém měl k dispozici záložní napájení na obvyklou dobu výpadku elektrické energie, například ve formě bezobslužných baterií. V případě delšího výpadku lze všechny dveře otevírat skupinovými klíči nebo generálním klíčem dostupným u ostrahy. Ostraha vede evidenci o požívání generálního klíče.

Systém je navržen tak, aby fungoval napříč všemi objekty společnosti ENERGETIKA a aby mohl být centrálně spravován. Tím však vzniká další úskalí. Přístupová oprávnění uživatelů se budou ověřovat vzdáleně na serveru, čímž může vzniknout značná latence, v případě výpadku linky i dočasné znemožnění přístupu zaměstnanců do objektů společnosti. Druhým problémem je nutnost napájet při výpadku dodávky elektrické energie i tuto komunikační linku (která může být přerušena ještě někde jinde na trase, kde to nejsme schopni ovlivnit). Řešením je použít v přístupovém systému jakýsi mezistupeň, který bude fungovat jako dočasné úložiště přístupových oprávnění, čímž se vyřeší jak problém latence, tak případná nestabilita linky.

Posledním zde jmenovaným nestandardním stavem je evakuace objektu v případě požáru nebo jiné katastrofy. V takovém případě musí být všem osobám v budově umožněno bezpečně budovu opustit. Všechny dveře označené jako nouzové východy se v případě požárního nebo jiného poplachu automaticky odjistí ve směru ven z budovy.

5 Zhodnocení a přínosy práce

Hlavním a zásadním přínosem této diplomové práce a v ní obsaženém návrhu přístupového systému pro společnost ENERGETIKA ČR, s.r.o je vytvoření jasných a jednotných pravidel přístupu do všech jednotlivých objektů společnosti.

Zavedení navrženého systému nebude mít pro společnost ENERGETIKA ČR, s.r.o. ani její dceřiné společnosti přímý ekonomický přínos. Tento systém bude zaváděn zejména z důvodů plnému vyhovění platné legislativě, co se týče ochrany prvků kritické infrastruktury. Hned na druhém místě je zájem společnosti ENERGETIKA ČR, s.r.o. chránit i ostatní svá aktiva dle nejnovějších a mezinárodně uznávaných standardů. Zavedení přístupového systému jako součásti fyzické ochrany dle ISMS popsaného v normách řady ČSN ISO/IEC 27000 se pak přímo nabízelo ze zjevných důvodů:

- Kybernetický zákon a jeho prováděcí vyhlášky říkají, že je-li subjekt certifikován dle normy ČSN ISO/IEC 27001, splňuje požadavky kybernetického zákona.
- Řada norem ČSN ISO/IEC 27000 se zabývá i ochranou jiných aktiv než prvků kritické infrastruktury, technické prostředky a pravidla popsaná v normách lze tak pohodlně použít na všechny objekty skupiny ENERGETIKA.
- Bude-li společnost ENERGETIKA ČR, s.r.o. a její dceřiné společnosti usilovat o certifikaci dle ČSN ISO/IEC 27001, přístupový systém již na tuto certifikaci bude plně připraven.

Byl vybrán jeden Modelový objekt v majetku skupiny ENERGETIKA, na kterém bylo ukázáno, jak by měl navržený přístupový systém v praxi fungovat. Realizace návrhu systému na tomto Modelovém objektu bude pilotním krokem postupného zavádění navrženého přístupového systému do všech objektů společnosti. Samotná realizace systému v Modelovém objektu bude provedena jako úprava stávajícího zabezpečovacího systému stávajícím dodavatelem zabezpečovacích služeb. Předpokládané náklady by se měly pohodlně vejít do finančního balíku určeného na provoz, údržbu a opravy zařízení budovy, díky čemuž nebude muset být vypisováno výběrové řízení a vedeno složité schvalovací řízení jako na investiční celek. Do budoucna je však nutné počítat s provozními náklady systému vyššími, než jsou stávající. Mimo jiné bude nutné proškolit pracovníky ostrahy objektů na používání nového systému.

Dalším přínosem pro společnost ENERGETIKA je snížení některých rizik, která hrozí s aktuálními přístupovými systémy. Co se zajisté podaří eliminovat?

- Před zavedením systému je možný téměř volný pohyb zaměstnanců i cizích osob po administrativních budovách, jakmile osoba projde přes vrátnici. To po zavedení přístupových zón nebude možné. Osoby se dostanou pouze do povolených prostor a nikam jinam. Tam budou stále pod dohledem zaměstnanců, za nimiž přišli řešit své záležitosti, nebo kamer.
- Revizí a posílením technických opatření fyzické ochrany dojde zároveň ke zvýšení bezpečnosti v areálech rozvoden, kdy posílená opatření ještě více odradí potenciálního útočníka od jeho zamýšleného chování, případně ho alespoň značně zdrží.
- Nový přístupový systém zcela jistě vyhovuje požadavkům platných zákonů na ochranu KI, tím se eliminuje riziko případné sankce ze strany státu.

Přístupový systém je navržen tak, aby byl dále rozšiřitelný pro další možné účely. Zcela jistě bude možné ho propojit s docházkovým systémem. Bezkontaktní karty přístupového systému by mohly být v budoucnu používány pro přístup do služebních vozidel (tuto technologii již nasadily některé společnosti poskytující sdílená vozidla).

Harmonogram průběhu realizace nového přístupového systému v rámci společnosti ENERGETIKA vypadá zhruba následovně:

- *Zadání projektu vedením*
- *Vytvoření, připomínkování a schválení osnovy projektu*
- Obstarání norem a předpisů
- Analýza současného stavu
- Návrh ochrany prvků KI a přístupového systému
- Porovnání současného a požadovaného stavu na pilotních objektech
- *Realizace změn na pilotních objektech*
- *Vyhodnocení pilotu*
- *Realizace na ostatních objektech skupiny.*

Jak je vidět z harmonogramu, tato diplomová práce řeší značnou část projektu zabezpečení KI a nového přístupového systému do objektů společnosti.

Závěr

Cílem této diplomové práce bylo navrhnout přístupový systém jako součást řešení fyzické bezpečnosti pro společnost ENERGETIKA ČR, s.r.o. a její dceřiné společnosti, jež je součástí nadnárodního energetického holdingu. Hlavním požadavkem na návrh tohoto systému je, aby plně vyhovoval všem zákonným požadavkům na ochranu prvků kritické infrastruktury, jelikož společnost takové prvky spravuje a je tedy subjektem kritické infrastruktury. Dalším požadavkem bylo navrhnout přístupový systém i pro ostatní objekty vlastněné nebo spravované společností. Jelikož je fyzická bezpečnost součástí bezpečnosti informací, padla volba na systém řízení bezpečnosti informací (ISMS) dle norem řady ČSN ISO/IEC 27000. Výhodou této volby je kompatibilita norem s požadavky zákonů České republiky, stačilo se tedy řídit normami a zákonné požadavky budou také plně splněny.

V teoretické části práce byly vyjmenovány a představeny právě příslušné normy a zákony související s předmětem této práce, velmi podrobně byl popsán proces řízení rizik dle normy ČSN ISO/IEC 27005 a také bylo popsáno řízení přístupu k aktivům.

Dále byla provedena analýza současného stavu. Po nutném představení společnosti následoval nelehký úkol klasifikovat objekty společnosti a na základě jasných kritérií je rozdělit do tříd. Pracovat se všemi jednotlivými objekty společnosti zvlášť by bylo nereálné. Následovaly analýzy současného stavu fyzické ochrany, a zvláště řízení přístupu. Zde jsem značně vycházel ze svých zkušeností nabytých při svých hojných návštěvách různých objektů společnosti. Práce pokračuje analýzami vnitřního i vnějšího prostředí a vyjmenováním kategorií některých rizik, která přináší současný stav.

Ve čtvrté kapitole byly nejdříve rozebrány identifikátory, jež je možné používat s přístupovými systémy a s přihlédnutím k požadavkům zadavatele byly vybrány ty nejvhodnější. Následně byl navržen a popsán přístupový systém pro jednotlivé třídy objektů a byla definována režimová opatření. Nakonec bylo popsáno, jak by měl být systém nasazen ve vybraném Modelovém objektu, ve kterém se setkává hned několik různých tříd budov.

V samotném závěru byl zhodnocen přínos této práce pro společnost ENERGETIKA a další možný budoucí vývoj, jak bude dále využita.

Citovaná literatura

1. **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.** *ČSN ISO/IEC 27000:2017 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

2. —. *ČSN ISO/IEC 27005:2013 Informační technologie – Bezpečnostní techniky – Řízení rizik bezpečnosti informací.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2013.

3. **Česká republika.** *Zákon č. 458/2000 Sb. o podmínkách podnikání a o výkonu státní správy v energetických odvětvích a o změně některých zákonů (energetický zákon) ze dne 28. listopadu 2000.*

4. **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.** *ČSN P 73 4450-1 Fyzická ochrana prvku kritické infrastruktury - Část 1: Obecné požadavky.* Praha : Fyzická ochrana prvku kritické infrastruktury - Část 1: Obecné požadavky, 2013.

5. **Česká republika.** *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) ze dne 23. července 2014.*

6. —. *Nařízení vlády č. 315/2014 Sb. o kritériích pro určení prvku kritické infrastruktury ze dne 8. prosince 2014.*

7. —. *Zákon č. 240/2000 Sb. o krizovém řízení a o změně některých zákonů (krizový zákon) ze dne 28. června 2000.*

8. **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.** *ČSN ISO/IEC 27001:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

9. —. *ČSN ISO/IEC 27000:2014 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Přehled a slovník.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

10. **Ondrák, Viktor, Sedlák, Petr a Mazálek, Vladimír.** *Problematika ISMS v mažerské informatice.* Brno : Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

11. **Česká republika.** *Zákon č. 22/1991 Sb. o technických požadavcích na výrobky a o změně a doplnění některých zákonů ze dne 24. ledna 1997.*

12. **International Organisation for Standardization.** *ISO/IEC 27000:2016 Information technology — Security texchniques — Information security management systems — Overview and vocabulary.* Ženeva : International Organisation for Standardization, 2016.

13. **Úřad pro technickou normalizaci, metrologii a státní zkušebnictví.** *ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy řízení bezpečnosti informací - Požadavky.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2006.

14. —. *ČSN ISO/IEC 27002:2014 Informační technologie - Bezpečnostní techniky - Soubor postupů pro opatření bezpečnosti informací.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2014.

15. —. *ČSN ISO/IEC 27003:2011 Informační technologie – Bezpečnostní techniky – Směrnice pro implementaci systému řízení bezpečnosti informací* . Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

16. —. *ČSN ISO/IEC 27004:2011 Informační technologie – Bezpečnostní techniky – Řízení bezpečnosti informací – Měření* . Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2011.

17. —. *ČSN ISO/IEC 27006:2016 Informační technologie – Bezpečnostní techniky – Požadavky na orgány provádějící audit a certifikaci systémů řízení bezpečnosti informací.* Praha : Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2016.

18. **International Organisation for Standardization.** *ISO/IEC TR 27019:2013 Information technology — Security techniques — Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.* Ženeva : International Organisation for Standardization, 2013.

19. **Česká republika.** *Nařízení vlády č. 432/2010 Sb. kritériích pro určení prvku kritické infrastruktury ze dne 22. prosince 2010.*

20. —. *Nařízení vlády č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, raktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) ze dne 15. prosince 2014.*

21. —. *Vyhláška č. 317/2014 Sb. o významných informačních systémech a jejich určujících kritériích ze dne 15. prosince 2014.*

22. —. *Zákon č. 101/2000 Sb. o ochraně osobních údajů a o změně některých zákonů ze dne 4. dubna 2000.*

23. **Evropská unie.** *Nařízení Evropského parlamentu a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) ze dne 27. dubna 2016* .

24. **Doucek, Petr, a další.** *Řízení bezpečnosti informací: Druhé rozšířené vydání o BCM.* Praha : Professional Publishing, 2011. ISBN 978-80-7431-050-8.

25. **Evropská Unie.** *Směrnice Evropského parlamentu a Rady 2009/72/ES ze dne 13. července 2009.*

26. **ENERGETIKA ČR, s.r.o.** Výroční zpráva ENERGETIKA ČR, s.r.o. 2015. [Online] 11. Březen 2016. [Citace: 3. Květen 2017.] https://www.ENERGETIKA.cz/-a70357?field=data.

27. **ENERGETIKA Prodej, a.s.** Výroční zpráva ENERGETIKA Prodej, a.s. 2015. [Online] 3. Květen 2016. [Citace: 3. Květen 2017.] https://www.ENERGETIKA.cz/-a59311?field=data.

28. **ENERGETIKA Distribuce, a.s.** Výroční zpráva ENERGETIKA Distribuce, a.s. 2015. [Online] 29. Březen 2016. [Citace: 3. Květen 2017.] https://www.ENERGETIKA.cz/-a63859?field=data.

29. **ENERGETIKA Servis, s.r.o.** Výroční zpráva ENERGETIKA Servis, s.r.o. 2015. [Online] 30. Březen 2016. [Citace: 3. Květen 2017.] https://www.ENERGETIKA.cz/-a63857?field=data.

30. **ENERGETIKA Výroba, s.r.o.** Výroční zpráva ENERGETIKA Výroba, s.r.o. 2014. [Online] 16. Červen 2015. [Citace: 3. Květen 2017.] https://www.ENERGETIKA.cz/-a15929?field=data.

31. **Počet obyvatel v regionech soudržnosti, krajích a okresech České republiky k 1. 1. 2016.** ***Český statistický úřad | ČSÚ.*** **[Online] 29. Duben 2016. [Citace: 2. Květen 2017.] https://www.czso.cz/documents/10180/32853387/1300721601.pdf.**

32. Rais, Karel a Doskočil, Radek. ***RISK MANAGEMENT, studijní text pro kombinovanou formu studia.*** **Brno : Akademické nakladatelství CERM, 2007. ISBN 978-80-214-3510-0.**

33. Burian, David. ***Provozování kamerových systémů: metodika pro splnění základních povinností ukládaných zákonem o ochraně osobních údajů.*** **Brno : Masarykova Univerzita pro Úřad pro ochranu osobních údajů, 2012. ISBN 978-80-210-6017-3.**

34. Deloitte Advisory, s.r.o. ***Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie.*** **Praha : Deloitte, 2012.**

Seznam použitých zkratek

Zkratka	Význam
1NP	1. Nadzemní podlaží
1PP	1. Podzemní podlaží
2NP	2. Nadzemní podlaží
a.s.	Akciová společnost
BOZP	Bezpečnost a ochrana zdraví při práci
BS	British Standard (Britská norma)
BT	Bezpečnostní třída
CCTV	Uzavřený televizní okruh/kamerový systém
CERT	Computer emergency response team
CNG	Compressed natural gas (stlačený zemní plyn)
COBIT	Control Objectives for Information and related Technology
ČB	Černobílý
ČR	Česká republika
ČSN	Česká technická norma
ČSÚ	Český statistický úřad
DPPC	Dohledová a poplachová přijímací centra
DS	Distribuční soustava
DTS	Detektor tříštění skla
EN	Evropská norma
EPS	Elektrická požární signalizace
ERÚ	Energetický regulační úřad
EU	Evropská unie
EZS	Elektronický zabezpečovací systém
FO	Fyzická ochrana
FOS	Fyzická ostraha
GDPR	General Data Protection Regulation

Zkratka	Význam
HR	Human resources (Lidské zdroje)
HZS	Hasičský záchranný sbor
ICT	Informační a komunikační technologie
ID	Identifikátor
IEC	International Electrotechnical Commission
IR	Infrared (infračervený)
ISBN	International standard book number
ISMS	Systém řízení bezpečnosti informací
ISO	International organization for Standardization
IT	Informační technologie
ITIL	Information Technology Infrastructure Library
IZS	Integrovaný záchranný systém
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
kV	Kilovolt (1000 V)
LAN	Local Area Network
LCD	Liquid Crystal Display
LOP	Lokalita, objekt, prostor
MK	Magnetický kontakt
MZP	Mechanické zábranné prostředky
NN	Nízké napětí
Obr.	Obrázek
OP	Občanský průkaz
PCO	Pult centralizované ochrany
PDCA	Demingův cyklus
PDS	Perimetrický detekční systém

Zkratka	Význam
PIN	Personal identification number
PIR	Pasivní infračervený detektor pohybu
PPN	Práce pod napětím
PPSZ	Poplachový přenosový systém
PVC	Polyvinylchlorid
PZS	Poplachový zabezpečovací systém
PZTS	Poplachový zabezpečovací a tísňový systém
s.r.o.	Společnost s ručením omezeným
Sb.	Sbírka (zákonů)
SBS	Soukromá bezpečnostní služba

Zkratka	Význam
SKV	Systém kontroly vstupů
SŘO	Systém řízení ochrany
STO	Systém technické ochrany
SWOT	Strenghts, Weaknesses, Opportunities, Threats
Tab.	Tabulka
ÚOOÚ	Úřad pro ochranu osobních údajů
VIS	Významný informační systém
VN	Vysoké napětí
VVN	Velmi vysoké napětí
WC	Toaleta

Seznam obrázků a grafů

Seznam tabulek

Seznam příloh

Příloha 1: Mechanické zábranné prostředky

Parametry FO		Parametry lokality, objektu, prostoru	Technické, režimové a organizační požadavky na FO
Perimetr areálu	Vnější oplocení	Konstrukce (mechanická odolnost)	kategorie "A" [1]
		Celková výška (vč. podhrabové přepážky nad terénem a mechanické zábrany na koruně)	min. 230 cm nad terénem
		Podhrabová deska	min. 10 cm nad terén min. 10 cm pod terén
		Mechanická zábrana na koruně	jednostranný nebo dvoustranný bavolet [2]
		Udržované pásmo (odstranění náletu)	min. 120 cm (na obě strany) [3]
	Vstupy	Způsob provedení vstupních branek	ručně otvíravá [4]
		Konstrukce (mechanická odolnost)	shodná s kategorií "A" konstrukce oplocení
		Celková výška (vč. mechanické zábrany na koruně)	min. 230 cm nad terénem
		Podhrabová deska – zpevněný povrch	min. 10 cm pod terén [5]
		Mechanická zábrana na koruně	jednostranný bavolet [2]
		Uzamykací systém nebo visací zámek	bezpečnostní třída 3 [6]
	Vjezdy	Způsob provedení hlavní vjezdové brány	s elektromotorickým pohonem [7]
		Způsob provedení ostatních vjezdových brán	ručně otvíravá [5]
		Konstrukce (mechanická odolnost)	shodná s kategorií "A" konstrukce oplocení
		Celková výška (vč. mechanické zábrany na koruně)	min. 230 cm nad terénem
		Podhrabová deska – zpevněný povrch	min. 10 cm pod terén [5]
		Mechanická zábrana na koruně	jednostranný bavolet [2]
		Uzamykací systém nebo visací zámek	neinstaluje se u brány s el. Pohonem, bezpečnostní třída 3 u brány ručně otvíravé [7]
	Budovy v perimetru	Pochůznou střechu budovy stejně vysoké nebo nižší než venkovní oplocení	prostředky MZP

Parametry FO		Parametry lokality, objektu, prostoru	Technické, režimové a organizační požadavky na FO
	Ostatní prostup	Funkční mříže	ano [8]
		Uzamykací systém nebo visací zámek	bezpečnostní třída 3 [6]
Vnější prostory	Oblast MZP	Venkovní stanoviště silového en. zařízení	v případě nemožnosti realizovat technické požadavky parametrů vnějšího oplocení perimetru objektu, realizovat tyto u venkovního stanoviště silového en. zařízení.
		Odstavné plochy vně objektu s uloženým majetkem (vozidla nebo materiál)	realizovat dle požadavku vlastníka [9]
		Vstupy do průchozích kabelových kanálů	realizovat dle požadavku vlastníka
Vnitřní prostory a budovy	Oblast MZP	Vstupní (venkovní) dveře a vrata v plášti budovy vč. nouzových východů a vstupů (do/z vnitřního prostoru budovy) z průchozích nebo průlezných abelových kanálů, resp. prostorů v PP budovy (konstrukce – mechanická odolnost)	dveře a vrata podle stanovených požadavků [10]
		Uzamykací systém nebo visací zámek ve vstupních (venkovních) dveřích a vratech do budovy	bezpečnostní třída 3 [11]
		Samouzavírací mechanismus na hlavních vstupních (venkovních) dveřích do budovy	ano [12]
		Prosklené části (dveře, okna) v plášti budovy, které jsou níže než 230 cm nad okolním terénem	funkční mříže nebo bezpečnostní fólie nebo bezpečnostní zasklení [13] / realizovat dle požadavku vlastníka
		Prosklené části (sklepní okna) v plášti budovy, které jsou pod úrovní okolního terénu, tzv. "anglický dvorek"	funkční mříže nebo bezpečnostní fólie nebo bezpečnostní zasklení [4] / realizovat dle požadavku vlastníka
		Další technické otvory v plášti budovy (s plochou větší než 600 cm2, které jsou níže než 230 cm nad okolním terénem nebo 120 cm od přístupové trasy)	funkční mříže [13] / realizovat dle požadavku vlastníka
		Pevné žebříky na plášti budovy vyúsťující na střechu	funkční mříž na úrovni střechy zabezpečená visacím zámkem v BT 3 [14] / realizovat dle požadavku vlastníka

Tabulka 1: Mechanické zábranné prostředky. Zdroj: Deloitte (34)

Příloha 2: Mechanické zábranné prostředky – kvalitativní požadavky

Číslo	Popis požadavku
[1]	- oplocení musí být sestaveno z plotových dílců, sloupků, - veškeré kovové díly v pozinkované struktuře, opatřené povrchovou ochranou z PVC (vypalovaný polyester např. fluidní metodou), vyjma žiletkového drátu. Oka budou provařována z důvodu uzemnění oplocení. Systém oplocení bude opatřen přípravkem pro uchycení - osová rozteč mezi jednotlivými sloupky nesmí být delší než 255 cm, - plotové dílce o velikosti oka max. 200 X 55 mm: - průměr drátu: Ø horizontálního drátu nesmí být menší než 8 mm, Ø vertikálního drátu nesmí být menší než 6 mm, Nebo - plotové dílce o velikosti oka max. 100 X 55 mm: průměr drátu: Ø horizontálního drátu nesmí být menší než 6 mm, Ø vertikálního drátu nesmí být menší než 5 mm, - sloupky musí být o Ø 60 mm nebo podobný rozměr např. 70X45, stěna sloupku nesmí být menší než 1,5 mm, plus pozinkování a PVC ochrana, - plotové dílce musí být uchyceny přímo do sloupku tak, aby bylo vyloučeno jejich vysunutí nebo jejich demontáž, - sloupky musí být vsazeny do země a spojeny z boku s opěrnými stěnami podhrabové desky min. čtyřmi kotvami nebo jinou obdobnou metodou (stabilizační držáky), aby nebylo možné oplocení demontovat. Základy budou z prefabrikovaných dílců, - životnost oplocení bez údržby, nesmí být nižší než 15 roků a musí být doložena Certifikátem VTÚO Brno nebo jiným akreditovaným ústavem. Nejlépe v ČR, nebo v českém jazyce, - mechanická odolnost musí být dodavatelem stanovena pevností v tahu a to min. odolnost proti tahu 400/550 N/mm², prodloužení max. 15 %, 40 g zinku / m². Doloženo certifikátem.
[2]	- jednostranný bavolet, osazený třemi řadami žiletkového drátu nebo dvoustranný bavolet osazený žiletkovou spirálou.
[3]	- udržované pásmo (odstraňování náletu) 120 cm po obou stranách vnějšího oplocení vybraného objektu, které zabrání v prorůstání vegetace a náletových dřevin oplocením, umožní se tím snadné odhalení poškození oplocení a také se tím znemožní možnost úkrytu
[4]	- mezera mezi spodní hranou vstupní branky a povrchem příjezdové komunikace nesmí umožnit podlezení ani podhrabaní případným narušitelem ani podlezení drobného zvířectva.
[5]	- mezera mezi spodní hranou vstupní branky a vjezdové brány a zpevněným povrchem příjezdové komunikace nesmí umožnit podlezení ani podhrabaní případným narušitelem a nesmí umožnit podlezení drobného zvířectva.
[6]	- dle ČSN EN 12320.

Číslo	Popis požadavku
	- bezpečnostní uzamykací systém – je tvořen bezpečnostním (zadlabacím) zámkem, bezpečnostní cylindrickou vložkou a bezpečnostním kováním. Vložka nebo kování musí chránit zámek proti odvrtání. - bezpečnostní visací zámek – je tvořen tvrzeným třmenem, cylindrickou vložkou nebo uzamykacím mechanismem odolným proti vyhmatání.
[7]	- pohon posuvné vjezdové brány – je navržen tak, aby bylo zamezeno možnému otevření brány (silou) bez použití identifikačního prostředku. - Dle ČSN EN 1627. - bezpečnostní uzamykací systém – je tvořen bezpečnostním (zadlabacím) zámkem, bezpečnostní cylindrickou vložkou a bezpečnostním kováním. Vložka nebo kování musí chránit zámek proti odvrtání. - bezpečnostní visací zámek – je tvořen tvrzeným třmenem, cylindrickou vložkou nebo uzamykacím mechanismem odolným proto vyhmatání.
[8]	- Funkční mříž musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN EN 1627.
[9]	- zabezpečuje se STO ve vazbě na hodnotu uloženého materiálu, resp. hodnoty parkujících dopravních a mechanizačních prostředků
[10]	- plné dveře, vrata, vjezdy (dále jen dveře) - musí být tuhé a pevné konstrukce, zhotovené z materiálu odolného proti vloupání (dřevo, plast, kov a jejich kombinace) o minimální tloušťce 40 mm.; - je-li výplň dveří kovová, musí být zhotovená z ocelového plechu o min. tloušťce 1 mm. - prosklené dveře – musí být, v jejich prosklených částech, zabezpečeny funkční mříží nebo bezpečnostní fólii nebo bezpečnostním zasklením nebo funkčním PZS. - dvoukřídlé dveře musí být zajištěny tak, aby obě křídla měla stejnou hodnotu odporu jako dveře jednokřídlé. Musí být zabezpečeny proti vyháčkování (pevné zástrče na neotvíraném křídle dveří, které jsou zajištěny šroubem s maticí nebo visacím zámkem, instalace příčné závory, instalace vzpěry neotvíravého křídla dveří). - vrata – musí být dostatečně tuhé a pevné konstrukce, zhotovené z plného plechu o min. tloušťce 3 mm, s rámem z ocelového profilu o min. tloušťce 5 mm, odolná proti vysazení a vyražení, s izolací. - funkční mříž musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN EN 1627. - bezpečnostní zasklení – vrstvené sklo nebo sklo s drátěnou vložkou musí vykazovat kategorii odolnosti min. třídy P5A podle ČSN EN 356, doloženo certifikátem. - bezpečnostní fólie – musí být instalována na skle s min. tloušťkou 4 mm. Po montáži fólie na sklo, musí sklo vykazovat kategorii odolnosti min. třídy P5A podle ČSN EN 356, doloženo certifikátem. Fólie musí být nalepena na vnitřní stranu skla a musí zasahovat až na jeho okraj
[11]	- dle ČSN EN 1627. - bezpečnostní uzamykací systém – je tvořen bezpečnostním (zadlabacím) zámkem, bezpečnostní cylindrickou vložkou a bezpečnostním kováním. - vložka nebo kování musí chránit zámek proti odvrtání. - bezpečnostní visací zámek – je tvořen tvrzeným třmenem, cylindrickou vložkou nebo uzamykacím mechanismem odolným proto vyhmatání.
[12]	- další vstupy do budovy vybavit samouzavíracím mechanismem dle požadavku vlastníka nebo uživatele objektu

Číslo	Popis požadavku
[13]	- funkční mříž musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN EN 1627. - bezpečnostní zasklení – vrstvené sklo nebo sklo s drátěnou vložkou musí vykazovat kategorii odolnosti min. třídy P5A podle ČSN EN 356, doloženo certifikátem. - bezpečnostní fólie – musí být instalována na skle s min. tloušťkou 4 mm. Po montáži fólie na sklo, musí sklo vykazovat kategorii odolnosti min. třídy P5A podle ČSN EN 356, doloženo certifikátem. Fólie musí být nalepena na vnitřní stranu skla a musí zasahovat až na jeho okraj
[14]	- funkční mříž musí splňovat požadavky bezpečnostní třídy 3 podle normy ČSN EN 1627. - bezpečnostní uzamykací systém – je tvořen bezpečnostním (zadlabacím) zámkem, bezpečnostní cylindrickou vložkou a bezpečnostním kováním. - vložka nebo kování musí chránit zámek proti odvrtání. - bezpečnostní visací zámek – je tvořen tvrzeným třmenem, cylindrickou vložkou nebo uzamykacím mechanismem odolným proti vyhmatání.

Tabulka 2: Mechanické zábranné prostředky – kvalitativní požadavky. Zdroj: Deloitte (34)

Příloha 3: PZTS, CCTV, SKV, PPSZ

Parametry FO		Parametry lokality – areálu, objektu – budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Perimetr areálu	Vnější oplocení	PZTS – perimetrická ochrana (PDS v oplocení nebo PDS podél oplocení uvnitř areálu)	ne nadstandard [1]
		Systém CCTV (s digitálním záznamem obrazového signálu)	ne nadstandard [1]
		Bezpečnostní osvětlení	ne nadstandard [1]
	Vstupy (vstupní branka)	Samouzavírací mechanismus (např. BRANO) se signalizací stavu	ano/ realizovat dle požadavku vlastníka
		Signalizace stavu otevření (v PZTS)	ano [2] / realizovat dle požadavku vlastníka
		Evidence vstupu (v PZTS nebo SKV)	ano [3]
		Monitorování a sledování vstupu (systém CCTV s digitálním záznamem obrazového signálu)	ano [4]
		Přenos stavů PZTS, SKV, CCTV na pracoviště en. dispečinku	ano [5]
		Přenos stavů PZTS, SKV, CCTV na dohledové pracoviště	ano
		Osvětlení vstupních branek	ano [6]
	Vjezdy (vjezdová a vlečková brána)	Světelná signalizace otvírání u hlavní vjezdové brány (MAJÁK – oranžová barva)	ano/realizovat dle požadavku vlastníka
		Signalizace stavu otevření hlavní vjezdové brány (v PZTS)	ano [2]
		Evidence vstupu / vjezdu u hlavní vjezdové brány (v PZTS nebo SKV)	ano [7]
		Monitorování a sledování vstupu / vjezdu u hlavní vjezdové brány (systém CCTV s digitálním záznamem obrazového signálu)	ano [4]
		Přenos stavů PZTS, SKV, CCTV na pracoviště en. dispečinku	ano [5]
		Přenos stavů PZTS, SKV, CCTV na dohledové pracoviště	ano
		Osvětlení vjezdových brán	ano [6]
Vnější prosto	PTZS	Odstavné plochy vně objektu s uloženým majetkem (vozidla nebo materiál)	realizovat dle požadavku vlastníka [8]

Parametry FO		Parametry lokality – areálu, objektu – budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
		Vstupy do průchozích kabelových kanálů uvnitř objektu	nerealizuje se PZS
	CCTV	Monitorování a sledování venkovního stanoviště silového zařízení uvnitř objektu	ne/nadstandard [9]
		Monitorování a sledování odstavné plochy vně objektu s uloženým majetkem (vozidla nebo materiál)	realizovat dle požadavků vlastníka
		Monitorování a sledování vstupů do průchozích kabelových kanálů uvnitř objektu	realizovat dle požadavků vlastníka
	SKV	Evidence vstupu ve venkovních prostorách objektu (v PZS nebo SKV)	nerealizuje se SKV
	PPSZ	Přenos poplachových a jiných funkčních stavů PZS na energetický dispečink	realizovat dle požadavků vlastníka/ řídicí systém MKD nebo datová síť LAN [10]
		Přenos poplachových a jiných funkčních stavů PZS na regionální dohledové pracoviště	realizovat dle požadavků vlastníka/ datová síť LAN nebo GSM [11]
Vnitřní prostory budov	PTZS	Vstupní (venkovní) dveře a vrata v plášti budovy vč. nouzových východů a vstupů (do/z vnitřního prostoru budovy) z průchozích nebo průlezných kabelových kanálů, resp. prostorů v PP budovy	realizovat dle požadavků vlastníka /prvky plášťové ochrany stupně zabezpečení 3 [12]
		Prosklené části (dveře, okna) v plášti budovy	realizovat dle požadavků vlastníka /prvky plášťové ochrany stupně zabezpečení 3 do 500 cm nad terén [13]
		Prosklené části (sklepní okna) v plášti budovy, které jsou pod úrovní okolního terénu, tzv. "anglický dvorek"	realizovat dle požadavků vlastníka /prvky plášťové ochrany stupně zabezpečení 3 [14]
		Prosklené části (dveře, okna) v plášti budovy přístupné z dosažitelných míst (pochůzné římsy a střechy, žebříky, balkony)	realizovat dle požadavků vlastníka / prvky plášťové ochrany stupně zabezpečení 3nad 500 cm nad terén [14]
		Další technické otvory v plášti budovy (s plochou větší než 600 cm2, které jsou níže, než je stanovená výška nad okolním terénem nebo 120 cm od přístupové trasy)	realizovat dle požadavků vlastníka / prvky plášťové nebo prostorové ochrany stupně zabezpečení 3 do 500 cm nad terén [15]
		Pevné žebříky na plášti budovy vyúsťující na střechu	realizovat dle požadavků vlastníka / prvky venkovní

Parametry FO		Parametry lokality – areálu, objektu – budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
			prostorové ochrany stupně zabezpečení 3 [16]
		Vyústění průchozího nebo průlezného kabelového kanálu (do/z vnitřního prostoru budovy)	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [17]
		Vyústění nouzového vylezu STOÚ (do/z vnitřního prostoru budovy)	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [18]
		Vstupní (vnitřní) dveře do prostorů, resp. místností související s provozem objektu	realizovat dle požadavků vlastníka / prvky plášťové ochrany stupně zabezpečení 3 [12]
		Prostory, resp. místnosti související s provozem objektu	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [19]
		Prostory, resp. místnosti související s provozem (řízením) objektu a nepřetržitou přítomností osob (stálá služba)	tísňový systém
		Vnitřní prostory u vstupních dveří do budovy (zádveří) a další společné prostory (chodby, schodiště)	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [20]
		Ostatní prostory nebo místnosti v budově na úrovni 1 NP budovy	realizovat dle požadavků vlastníka / prvky prostorové ochrany stupně zabezpečení 3 [20]
		Prostor nebo místnost s instalovanou ústřednou PZTS	realizovat dle požadavků vlastníka / prvky plášťové a prostorové ochrany stupně zabezpečení 3 [21]
	CCTV	Monitorování a sledování vstupů do budovy, pláště budovy a vybraných vnitřních prostor budovy systémem CCTV (s digitálním záznamem obrazového signálu)	ne, nadstandard [22] / realizovat dle požadavků vlastníka
	SKV	evidence vstupu do budovy (v PZTS nebo SKV)	realizovat dle požadavků vlastníka / ano [23]

Parametry FO		Parametry lokality – areálu, objektu – budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
		evidence vstupu do vybraných prostor nebo místnosti souvisejících s provozem objektu (v PZTS nebo SKV)	ano [23]
	PPZS	přenos poplachových a jiných funkčních stavů PZTS na energetický dispečink	realizovat dle požadavků vlastníka / řídicí systém MKD nebo datová síť LAN [24]
		přenos poplachových a jiných funkčních stavů PZTS na regionální dohledové pracoviště	realizovat dle požadavků vlastníka / datová síť LAN nebo GSM, [25]

Tabulka 3: PZTS, CCTV, SKV, PPSZ. Zdroj: Deloitte (34)

Příloha 4: PZTS, CCTV, SKV, PPSZ – kvalitativní požadavky

Číslo	Popis požadavku
[1]	- dle požadavků vlastníka objektu
[2]	- MK stupně zabezpečení 3 - střední až vysoké riziko dle ČSN EN řady 50 131.
[3]	- ovládacím prvkem je oboustranný bezkontaktní snímač identifikačních prostředků. - ovládacím prostředkem je karta. - evidence je součástí PZS.
[4]	- monitorovat kamerami venkovního sledovacího systému CCTV s digitálním záznamem obrazového signálu (dle ČSN EN 50 132-7) a to: - venkovní pevné barevné digitální kamery s vysokým rozlišením a citlivostí a s možností přepnutí do ČB módu v provedení „antivandal“, instalované na exponovaných místech na základě provedených kamerových zkoušek. - přenos videosignálu v digitalizované formě po datové síti LAN realizovat na dohledové pracoviště.
[5]	- přenos pouze stavů PZTS.
[6]	- pochůzkové osvětlení uvnitř perimetru objektu, zaměřené na osvětlení hlavního vstupu a vjezdu a v prostoru kolem budovy společných provozů.
[7]	- ovládacím prvkem jsou bezkontaktní snímače identifikačních prostředků umístěné na vjezdu a výjezdu. - ovládacím prostředkem je karta, dálkový ovládač, mobilní telefon. - evidence je součástí PZTS.
[8]	- zabezpečuje se STO ve vazbě na hodnotu uloženého materiálu, resp. hodnoty parkujících dopravních a mechanizačních prostředků
[9]	- dle požadavků vlastníka objektu - monitorovat kamerami venkovního sledovacího systému CCTV s digitálním záznamem obrazového signálu (dle ČSN EN 50 132-7) a to: - venkovní pevné barevné digitální kamery s vysokým rozlišením a citlivostí a s možností přepnutí do ČB módu v provedení antivandal, instalované na exponovaných místech na základě provedených kamerových zkoušek. - přenos videosignálu v digitalizované formě po datové síti LAN realizovat na dohledové pracoviště.
[10]	- na dispečerské pracoviště realizovat přenos stavu PZTS v rozsahu min. signalizace vyhlášení poplachového stavu a informace o aktivním, resp. neaktivním stavu PZTS.
[11]	- optickou a akustickou signalizaci jednotlivých stavů PZTS realizovat prostřednictvím přenosového zařízení na dohledové pracoviště
[12]	- MK dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - MK instalovat na všech otvíravých křídlech dveří a vrat.
[13]	- MK dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - MK instalovat na všech otvíravých křídlech dveří a vrat. - použití prvků PZTS dle konstrukčního řešení prosklených části v plášti budovy.
[14]	- MK a DTS dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko

Číslo	Popis požadavku
	- použití prvků PZTS dle konstrukčního řešení prosklených části v plášti budovy
[15]	- MK nebo DTS nebo PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko - použití prvků PZS dle stavebně technického řešení technického otvoru.
[16]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - instalovat na pochůzné střeše budovy v místě vyústění žebříku.
[17]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - instalovat před vstupem do vnitřního prostoru budovy (uvnitř kabelového prostoru).
[18]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - instalovat uvnitř místnosti před vstupem do nouzového vylezu.
[19]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - instalovat před vstupem do vnitřního prostoru (energetický dispečink, systém kontroly řízení apod.).
[20]	- PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko.
[21]	- MK, DTS a PIR dle ČSN EN řady 50 131 stupně zabezpečení 3 - střední až vysoké riziko. - MK instalovat na všech otvíravých křídlech dveří a vrat.
[22]	- dle požadavků vlastníka objektu - monitorovat kamerami venkovního sledovacího systému CCTV s digitálním záznamem obrazového signálu (dle ČSN EN 50 132-7) a to: - venkovní pevné barevné digitální kamery s vysokým rozlišením a citlivostí a s možností přepnutí do ČB módu v provedení antivandal, instalované na exponovaných místech na základě provedených kamerových zkoušek. - přenos videosignálu v digitalizované formě po datové síti LAN realizovat na dohledové pracoviště.
[23]	- ovládacími prostředky prvků plášťové a prostorové ochrany PZTS jsou bezkontaktní identifikační karty typu Mifare, případně karty jiného typu užívané v oblasti výroby, přenosu a distribuce el. energie - ovládacími prvky jsou bezkontaktní snímače identifikačních prostředků, které musí být kompatibilní s technologií používané karty. Instalují se na plášti budovy, zabezpečené PZTS u hlavního vstupu do budovy a dále dle požadavku vlastníka objektu - kódová LCD klávesnice (uživatelská) se instaluje u vstupu do budovy společných provozů a dalších budov dle požadavku vlastníka objektu – evidence je součástí PZTS.
[24]	- na dispečerské pracoviště realizovat přenos stavu PZTS v rozsahu min. signalizace vyhlášení poplachového stavu a informace o aktivním, resp. neaktivním stavu PZTS.
[25]	- optickou a akustickou signalizaci jednotlivých stavů PZTS

Tabulka 4: PZTS, CCTV, SKV, PPSZ – kvalitativní požadavky. Zdroj: Deloitte (34)

Příloha 5: Režimová opatření

Parametry RO	Parametry lokality – areálu, objektu – budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Parametry vztahující se k RO	Stanovení určených vstupů pro osoby a vjezdů pro vozidla do objektu	Režimová opatření týkajících se objektu zpracovává vlastník objektu interním pracovním dokumentem (Řád fyzické ochrany) tak, aby minimálně všechny zmíněné oblasti byly pokryty.
	Stanovení rozsahu oprávnění osob pro vstup a dopravních prostředků pro vjezd do objektu	
	Režim pohybu osob, vozidel v objektu	
	Režim pohybu materiálu v objektu (vnášení, vynášení majetku)	
	Režim manipulace s klíči	
	Režim manipulace se STO	
	Řešení mimořádných událostí (bezpečnostní incidenty, teroristické výhrůžky)	

Tabulka 5: Režimová opatření. Zdroj: Deloitte (34)

Příloha 6: Fyzická ostraha

Parametry FOS	Parametry lokality – areálu, objektu – budovy, prostoru (LOP)	Technické, režimové a organizační požadavky na parametry FO v LOP
Parametry vztahující se k FOS	Výkon stálé služby na objektu	ne / ano [1]
	Obchůzková činnost na objektu (pravidelná nebo nepravidelná)	ne nadstandard [2]
	Strážní činnost na objektu bez instalovaného STO (pravidelná nebo nepravidelná)	realizovat dle požadavků vlastníka / ano [3]
	Obsluha STO na dohledovém pracovišti (nepřetržitě)	ano
	Vyhodnocování stavů STO a reakce na ně (průběžné)	ano [4]
	Mobilní zásah na objektu (neprodleně)	ano [5]

Tabulka 6: Fyzická ostraha. Zdroj: Deloitte (34)

Příloha 7: Fyzická ostraha – kvalitativní požadavky

Číslo	Popis požadavku
[1]	- výkon stálé služby na objektu bude realizován po omezenou dobu v případě, že bude probíhat realizace celkové obnovy, resp. rekonstrukce objektu spojené s rekonstrukcí vnějšího oplocení.
[2]	- lze nadstandardně realizovat, a to v případě, že se objekt nachází v bezprostřední blízkosti objektu se stálým stanovištěm fyzické ostrahy a souhlasu vlastníka objektu.
[3]	- fyzická kontrola stavu (neporušenosti) vnějšího oplocení, pláště budov v objektu. – odvrácení vzniku majetkové újmy
[4]	- spolupráce s dispečerem dispečinku, uživatelem a vlastníkem objektu, Policii ČR, HZS apod.
[5]	- činnost zásahové skupiny na objektu při vyhlášených poplachových stavech STO (výjezdové vozidlo SBS). - odvrácení vzniku majetkové újmy a zadržení narušitele.

Tabulka 7: Fyzická ostraha – kvalitativní požadavky. Zdroj: Deloitte (34)

Příloha 8: Katalog hrozeb kritické infrastruktury z oblasti výroby, přenosu a distribuce elektrické energie

Skupina	Hrozba
Přírodní hrozby	Blesk
	Elektromagnetická radiace
	Kroupy
	Námraza
	Pád stromu
	Povodeň
	Požár
	Přívalový déšť
	Sesuv půdy
	Sníh
	Vichřice
	Vysoká teplota
	Zemětřesení
	Znečistěné ovzduší prachem
Technické hrozby	Jaderná havárie
	Provozní porucha
	Přerušení dodávky elektřiny
	Přerušení dodávky vody
	Rozsáhlé nehody vně prostoru
	Selhání klimatizace
	Selhání osvětlení v posuzovaném prostoru
	Selhání topení
	Selhání záložních zdrojů napájení
	Únik a výbuch plynu mimo prostor
	Únik ropných látek mimo prostor
	Únik ropných látek v prostoru
	Únik vody z vod. Řadu mimo prostor
	Únik vody z vod. Řadu v prostoru
	Zamoření ovzduší nebezpečným plynem
Technické selhání systém	Porucha kabeláže
	Porucha pracovní stanice

Skupina	Hrozba
	Porucha prvku CCTV
	Porucha prvku PTZS
	Porucha prvku SKV
	Porucha serveru
	Porucha zámkových systémů
	Selhání software
Lidský faktor – organizační selhání	Chybná manipulace s prvky systému fyzické ochrany
	Nedbalost, ignorance pracovníků
	Nedodržení pracovních postupů
	Nedostatek lidských zdrojů
	Nedostatek materiálních zdrojů
	Nevhodně stanovené pracovní postupy
	Neznalost, nepřipravenost zaměstnanců
	Provozní chyba pracovníků třetích stran
	Provozní chyba zaměstnanců
	Selhání bezpečnostní služby
Lidský faktor – ohrožení fyzické povahy	Demonstrace v blízkosti prostor
	Destrukce prostor nebo jejich části
	Krádež provedená cizími osobami
	Krádež provedená pracovníky třetích stran
	Krádež provedená zaměstnancem
	Násilné vniknutí cizí osoby do prostor
	Neoprávněná manipulace s prvky systému fyzické ochrany
	Neoprávněný přístup cizí osoby do prostoru
	Neoprávněný přístup k prvkům systému fyzické ochrany
	Odezírání při kódování a přihlášení do systému fyzické ochrany
	Odposlech komunikace prvků systému fyzické ochrany
	Použití zbraně / loupežné přepadení
	Předstírání fyzické identity cizími osobami
	Předstírání fyzické identity pracovníky třetích stran
	Předstírání fyzické identity zaměstnancem
	Předstírání uživatelské identity
	Sabotáž zaměstnance
	Úmyslné poškození bezpečnostních prvků

Skupina	Hrozba
	Úmyslné poškození prostoru cizí osobou
	Úmyslné poškození prostoru zaměstnancem
	Vloupání do prostor
	Získání informací o ochraně prostoru
	Zničení bezpečnostních prvků prostor
	Zničení chladícího zařízení
	Zničení venkovního vedení – lana
	Zničení venkovního vedení – sloupy
	Zničení vod. řadu
Lidský faktor – terorismus	Dopisní a balíkové zásilky s nebezpečným obsahem
	Držení rukojmí
	Použití otravných prostředků pracoviště
	Únos zaměstnanců
	Vydírání zaměstnanců
	Výhrůžky – ostatní
	Výhrůžky napadení Elektrické stanice a stálé služby Zničení nebo vyřazení technologických prostorů pro zpracování a přenos dat
	Výhrůžky napadení Hlavního dispečerského
	Výhrůžky umístnění bomby – písemně
	Výhrůžky umístnění bomby – telefonicky, e-mailem
	Zničení nebo vyřazení dispečerského pracoviště
	Zničení nebo vyřazení pracoviště stálé služby
logické hrozby	Falšování uživatelské identity cizími osobami
	Falšování uživatelské identity identifikovatelnými
	Falšování uživatelské identity smluvními
	Neoprávněné použití aplikace osobami
	Zavedení destruktivních a škodlivých programů poskytovateli služeb
	Zneužití systémových prostředků
Komunikační hrozby	Chybné směrování
	Infiltrace komunikace
	Manipulace komunikace
	Odmítnutí odpovědnosti
	Selhání komunikace
	Začlenění škodlivých programů

Skupina	Hrozba
	Zachycení komunikace
Závady zařízení	Selhání aplikačního programového vybavení
	Selhání klimatizace
	Selhání napájení
	Selhání systémového nebo síťového programového vybavení
	Technická závada paměťového zařízení
	Technická závada počítače
	Technická závada počítače pro řízení / správu sítě
	Technická závada síťové brány
	Technická závada síťové služby
	Technická závada síťového distribučního prvku
	Technická závada síťového rozhraní
	Technická závada tiskového zařízení
Chyby	Chyba údržby technického vybavení
	Chyba úpravy programového vybavení
	Chyba uživatele
	Provozní chyba
Fyzické hrozby	Krádež provedená cizími osobami
	Krádež provedená identifikovatelnými osobami
	Nedostatek personálu
	Poškození vodou
	Požár
	Přírodní katastrofa
	Terorismus
	Úmyslné poškození cizími osobami
	Úmyslné poškození identifikovatelnými osobami

Tabulka 8: Katalog hrozeb. Zdroj: Deloitte (34)

Příloha 9: Soupis všech místností modelového objektu

Budova	Podlaží	Označení	Popis
Doprava	1PP	0.01	WC Muži
		0.02	WC Ženy
		0.03	Chodba
		0.04	Sprcha
		0.05	Archiv
		0.06	Úklid
	1NP	1.01	Obchodní kancelář
		1.02	Garáže
		1.03	Chodba + schodiště
		1.04	Kuchyňka
		1.05	Chodba
		1.06	WC
		1.07	WC
		1.08	Chodba
		1.09	Kancelář vedoucí
		1.10	Kancelář manažeři
		1.11	Chodba
		1.12	Kancelář manažer
		1.13	Garáž – měřící vůz
		1.14	Schodiště
		Chodba	Chodba
		Kancelář	Kancelář
		kancelář	Kancelář
		Kancelář	Kancelář
		Sklad	Sklad
	2NP	2.01	Koordinátor PPN
		2.02	Vedoucí montérů PPN
		2.03	Kancelář měřící vůz
		2.04	Šatna
		2.05	Sprcha
		2.06	WC

Budova	Podlaží	Označení	Popis
		2.07	WC
		2.08	Kuchyňka
		2.09	Chodba
		2.10	Chodba + schodiště
		2.11	Montéři PPN
Rozvodna	1PP	0.1	Chodba
		0.2	Sklad
		0.3	Sklad
		0.4	Rozvodna VN
		0.5	Sklad
		0.6	Sklad
		0.7	Sklad
		0.8	Rozvodna VN
		0.9	Sklad
		0.10	Trafokomora
		0.11	Trofokomora
		0.12	Dopravní šachta
	1NP	1.1	Zádveří
		1.2	Schodiště
		1.3	Rozvodna VN
		1.4	Kancelář
		1.5	Kancelář
		1.6	Kancelář
		1.7	Kancelář
		1.8	Rozvodna VN
		1.9	Rozvaděč NN
		1.10	Kancelář
		1.11	Kancelář
		1.12	WC
		1.13	Umývárna
		1.14	Zádveří
		1.15	Dispečink Rozvodny
		1.16	Kancelář
		1.17	WC

Budova	Podlaží	Označení	Popis
		1.18	Umývárna
	2NP	2.1	Chodba + schodiště
		2.2	Kuchyňka
		2.3	Kancelář
		2.4	Kancelář
		2.5	Kancelář
		2.6	Kancelář
		2.7	Kancelář
		2.8	Kancelář
		2.9	Kancelář
		2.10	Kancelář
		2.11	WC Ženy
		2.12	WC Muži
		2.13	Úklid
		2.14	Zasedací místnost
		2.15	Kuchyňka
		2.16	Zasedací místnost
		2.17	Kancelář
		2.18	Kancelář
		2.19	Chodba
Služebna	1PP	Garáž	Garáž
		Garáž	Garáž
		Garáž	Garáž
		Schodiště	Schodiště
		Sklad	Sklad
		Sklad	Sklad
	1NP	13	Kancelář
		14	Kancelář
		15	Kancelář
		16	Kancelář
		17	Kancelář
		18	Kancelář
		Chodba	Chodba
		Schodiště	Schodiště

Budova	Podlaží	Označení	Popis
		Šatna	Šatna
		WC	WC
		WC	WC

Tabulka 9: Soupis místností Modelového objektu. Zdroj: Vlastní